# AUTOMORPHISMS OF CARTAN MODULAR CURVES OF PRIME AND COMPOSITE LEVEL

VALERIO DOSE, GUIDO LIDO, AND PIETRO MERCURI

Abstract. We study the automorphisms of modular curves associated to Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and certain subgroups of their normalizers. We prove that if $n$ is large enough, all the automorphisms are induced by the ramified covering of the complex upper half-plane. We get new results for non-split curves of prime level $p \geqslant 13$: the curve $X_{\mathrm{ns}}^{+}(p)$ has no non-trivial automorphisms, whereas the curve $X_{\mathrm{ns}}(p)$ has exactly one non-trivial automorphism. Moreover, as an immediate consequence of our results we compute the automorphism group of $X_0^*(n) := X_0(n)/W$, where $W$ is the group generated by the Atkin-Lehner involutions of $X_0(n)$ and $n$ is a large enough square.

## Introduction

Since the 1970s many efforts have been made to determine automorphisms of modular curves and in particular to establish whether a modular curve has other automorphisms besides the expected ones. Indeed, infinite automorphisms naturally arise when the curve has genus zero or one. Moreover, since the components of modular curves over $\mathbb{C}$ can be seen as compactification of quotients of the complex upper half-plane $\mathbb{H}$, some automorphisms of $\mathbb{H}$ induce automorphisms of the quotient modular curve. Such automorphisms are called *modular* and their determination is a purely group theoretic problem.

The focus has been classically placed on the modular curves $X_0(n)$ associated to a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (e.g., upper triangular matrices), with $n$ a positive integer. For these curves, modular automorphisms played an important role in the development of the theory of modular curves. They were determined in the seminal paper [AL70], with a small gap which was later filled in a couple of different ways (see [AS90], [Bar08]). Meanwhile, a complete picture about the remaining automorphisms of $X_0(n)$ has been painted through the decades by the works [Ogg75a], [Ogg77], [KM88], [Elk90], [Har11]. Also some works in this century (e.g., [BH03], [Mer18], [Gon16]) took on the case of the modular curves $X_0(p)/\langle w_p\rangle$ and $X_0(p^2)/\langle w_{p^2}\rangle$, where $w_p$ and $w_{p^2}$ are the Atkin-Lehner involutions of the respective modular curve.

More recently, great interest has been generated in modular curves associated to different subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, in particular to normalizers of Cartan subgroups for $n = p$ prime. This is mainly due to the fact that rational points on these curves help classifying rational elliptic curves whose associated Galois representation modulo $p$ is not surjective. This is directly linked to a question formulated by Serre (also known as *uniformity conjecture*) in the 1970s ([Ser72]). After the works [Maz78], on the Borel case, and [BP11],

2010 *Mathematics Subject Classification.* 14G35,11G18,11G30,11G05,11G15.

*Key words and phrases.* modular curves, elliptic curves, complex multiplication, automorphisms.

The third author has been supported by the research grant “Ing. Giorgio Schirillo” of the Istituto Nazionale di Alta Matematica “F. Severi”, Rome. We would also like to thank Claudio Stirpe, for giving us access to some of his source code which we used for this work, and the anonymous Referee, for the very careful reading and for the many useful comments.

[BPR13], on the *split* Cartan case, the only part of this problem left to understand nowadays is equivalent to asking whether, for almost every prime $p$, the modular curve $X_{\mathrm{ns}}^{+}(p)$ associated to the normalizer of a *non-split* Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has other rational points besides the expected ones, namely the CM points of class number one. This equivalence led to a certain amount of research driven towards computing equations and finding rational points of modular curves associated to non-split Cartan subgroups and their normalizers (see for example [Bar09], [Bar14], [BDM$^+$19], [DFGS14], [DMS19], [MS20]).

A curious connection between the problem of determining rational points and the one of determining automorphisms in a modular curve is given by the fact that in the case of the Borel modular curves $X_0(p)$ of genus at least 2, the sole occurrence of unexpected rational points ($p = 37$) in the setting of Serre's uniformity conjecture, happens in the presence of an unexpected automorphism of the corresponding modular curve. A further connection is made in [Dos16], where is proven that, for $p \geqslant 29$, the absence of unexpected rational points of the curve $X_{\mathrm{ns}}^{+}(p)$ implies the absence of unexpected rational automorphisms of the modular curve $X_{\mathrm{ns}}(p)$ associated to a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

The first work centered on automorphisms of non-split Cartan modular curves has been [DFGS14], in which the existence of an unexpected automorphism of $X_{\mathrm{ns}}(11)$ is proven. Some partial results on the automorphisms of $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^{+}(p)$, for almost every prime $p$, were proven in [Dos16], while in [Gon17] the full determination of the automorphism group is obtained for low primes ($p \leqslant 31$).

In the present work, we prove unconditionally that every automorphism of $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^{+}(p)$ is modular for $p \geqslant 13$. In fact, we also extend this to composite level $n$ where we can define Cartan subgroups of mixed split/non-split type. The scope of our study concerns Cartan subgroups and also a specific subgroup of their normalizer in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which we call *Cartan-plus* subgroup. However, in most cases, for example when $n$ is odd, a Cartan-plus subgroup actually coincides with the normalizer of the relative Cartan subgroup. We prove the following result:

**Theorem 5.8.** *Let $n \geqslant 10^{400}$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of $X_H$ is modular, hence we have*

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at 2,} \\ N'/H', & \text{otherwise,} \end{cases}$$

*where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.*

The huge bound of $10^{400}$ comes from Proposition 4.7 hence from our estimates of the dimension of the CM part of $J_0(n)$. However, explicit computations can make the method work for low levels (see Table 6.1 in the Appendix). It may be interesting to note that the modular curve associated to a Cartan-plus subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which is split at every prime dividing $n$ is isomorphic to the modular curve $X_0^*(n^2) := X_0(n^2)/W$, where $W$ is the group generated by Atkin-Lehner involutions of the Borel curve $X_0(n^2)$. For these curves, the case where $n$ is squarefree has been recently determined in [BG].

In the case $n = p^e$, where $p$ is a prime number, we can refine the techniques developed and obtain a more complete result:

**Theorem 5.11.** *Let $p$ be a prime number and let $e$ be a positive integer. If $p^e > 11$ and $p^e \notin \{3^3, 2^4, 2^5, 2^6\}$, then all the automorphisms of $X_{\mathrm{ns}}(p^e)$, $X_{\mathrm{ns}}^{+}(p^e)$, $X_{\mathrm{s}}(p^e)$ and $X_{\mathrm{s}}^{+}(p^e)$ are* *modular and*

$$\mathrm{Aut}(X_{\mathrm{ns}}(p^e)) \cong \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{Aut}(X_{\mathrm{ns}}^+(p^e)) \cong \{1\},$$

$$\mathrm{Aut}(X_{\mathrm{s}}(p^e)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3, \end{cases} \quad \mathrm{Aut}(X_{\mathrm{s}}^+(p^e)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3, \\ \{1\}, & \text{if } p > 3, \end{cases}$$

*where the above semidirect product* $(\mathbb{Z}/8\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ *is described in Table 5.1.*

**Corollary 5.12.** *Let* $p \geqslant 13$ *be a prime number. Then the group of automorphisms of* $X_{\mathrm{ns}}^+(p)$ *is trivial and the group of automorphisms of* $X_{\mathrm{ns}}(p)$ *has order* 2.

The idea of the proof is the following. We start by showing that an automorphism $u$ of $X_H$ is defined over some explicit compositum of quadratic fields. This is done by studying the endomorphisms of the jacobian of $X_H$, which, through an isogeny relation, can be seen as endomorphisms of the well known modular jacobians $J_0(n)$. The fact that $u$ is defined over a compositum of quadratic fields, together with the Eichler-Shimura Relation, allow us to show that $u$ "almost" commutes with the Hecke operators. We can then describe the action of Hecke operators on cusps and branching points of the cover $\mathbb{H} \to X_H$, and prove that $u$ preserves both these sets. This allows to lift $u$ to an automorphism of $\mathbb{H}$.

The main technical novelty of our proofs is the analysis of the action of Hecke operators mentioned above, which permits us to prove the result about automorphisms without exploiting and worrying about the field of definition of the cusps and CM points, which has been instead instrumental for determining automorphisms of modular curves throughout the literature in the past. In fact, both [KM88] and [Dos16] use the field of definition of the cusps to prove that an automorphism must preserve the set of cusps. In [KM88], this is enough to exclude the existence of non-modular automorphisms, in combination with the rich action of the modular automorphisms of $X_0(n)$ on the set of cusps. In [Dos16], the lack of the preservation result on the set of branching points confines the analysis to the levels where there are no branching points at all. We also give à la Chen results to describe jacobians of Cartan modular curves in terms of jacobians of Borel modular curves and we give an explicit upper bound on the dimension of the CM part of the jacobian of Borel modular curves.

The structure of the paper is the following.

In Section 1 we define modular curves associated to general subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and we give an equivalent condition to the fact that a point of a modular curves branches in the covering of the curve by $\mathbb{H}$.

In Section 2 we study the action of Hecke operators on modular curves. In particular we focus on the action on the cusps and the other points which could branch in the covering by $\mathbb{H}$. Such points are associated to elliptic curves with $j$-invariant equal to 0 or 1728.

In Section 3 we define Cartan and Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for every positive integer $n$. We also define the relative modular curves of composite level. Then we prove that the jacobian of a Cartan modular curve is a quotient of the jacobian of some Borel modular curve. When $n = p^e$, this is done applying the techniques of [Che04] and [dSE00] to a previously unexplored case, and for $n$ general we combine these results. We also extend the results of [Che04] to the case of even level.

In Section 4 we prove that all the automorphisms of Cartan modular curves must be defined on a compositum of quadratic fields when the level $n$ is large enough. To do this, we use a geometrical criterion that we can apply by bounding the dimension of the

CM part of the jacobian of Cartan modular curves. This last step is obtained using the isogenies of Section 3 and computing explicit bounds for the CM part of the jacobians of Borel modular curves. Furthermore, we refine the results in the case $n = p^e$, with $p$ prime.

Finally, in Section 5 we prove the results stated above about automorphisms. After showing that each automorphism must preserve the cusps and the set of branching points of the covering by $\mathbb{H}$, we prove that there are no non-modular automorphisms. Thus, we compute the modular automorphisms to complete the analysis and we discuss their field of definition. We first concentrate on Cartan modular curves of general level $n$. Then we adapt the strategy to the case $n = p^e$, with $p$ prime, giving the complete result for $X_{\mathrm{ns}}(p)$ and $X^+_{\mathrm{ns}}(p)$, and improving the result we obtained for the general level in the cases of $X^+_{\mathrm{s}}(p^e)$, $X_{\mathrm{ns}}(p^e)$ and $X^+_{\mathrm{ns}}(p^e)$. To treat some of the small level cases, we use the criterion of [Gon17] and some ad hoc arguments which we verify through an algorithm implemented in MAGMA ([BCFS]) which is available at [Scr].

As we did for the case of level $n = p^e$, with $p$ prime in Theorem 5.11, the result on Cartan modular curves of composite level can be sharpened, with our techniques, for levels with a specific type of factorization. However, certain cases remain out of the reach of the strategy described in this work: for example when we are not able to complete the argument using the criterion of [Gon17] and either we have a low gonality lower bound for the modular curve (e.g., $X_{\mathrm{ns}}(16)$, $X^+_{\mathrm{ns}}(27)$, $X_{\mathrm{ns}}(27)$, $X^+_{\mathrm{ns}}(32)$, $X_{\mathrm{ns}}(32)$, $X^+_{\mathrm{ns}}(64)$) or its jacobian has a large CM part relative to its dimension (see Remark 4.11 for the example with the lowest level). A table with the relevant data for the totally split or totally non-split curves of level $n \leqslant 64$, and the description of a few cases having exceptional automorphisms, can be found in the Appendix.

## 1. Modular curves

Let $n$ be a positive integer. We denote by $Y(n)$ the (coarse if $n < 3$) moduli space that parametrizes pairs $(E, \phi)$ where $E$ is an elliptic curve over a $\mathbb{Q}$-scheme $S$ and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2_S \to E[n]$ is an isomorphism of $S$-group schemes. We denote by $X(n)$ the compactification of $Y(n)$ and we call $X(n)$ the *modular curve of full level n*.

Every matrix $\gamma \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ gives an automorphism of the constant group scheme $(\mathbb{Z}/n\mathbb{Z})^2_S$, hence $\gamma$ acts on $Y(n)$ sending $(E, \phi)$ to $(E, \phi \circ \gamma)$. This defines an action of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ on $Y(n)$ that extends uniquely to $X(n)$. For each subgroup $H$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let $X_H$ be the quotient $X(n)/H$. By [DR73, IV.6.7], $X_H$ has good reduction over each prime that does not divide $n$ and the smooth model of $Y_H = Y(n)/H$ over $\mathbb{Z}[1/n]$ is a coarse moduli space for *elliptic curves with $H$-structure*, i.e., the equivalence classes of pairs $(E, \phi)$ where $E$ is an elliptic curve over a $\mathbb{Z}[1/n]$-scheme $S$ and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2_S \to E[n]$ is an isomorphism of $S$-group schemes, and the equivalence relation is given by:

$$(E, \phi) \sim_H (E', \phi') \iff (\phi')^{-1} \circ \iota|_{E[n]} \circ \phi = h, \text{ for some } h \in H \text{ and } \iota\colon E \xrightarrow{\sim} E'. \tag{1.1}$$

In particular, for every algebraically closed field $K$ of characteristic $p \nmid n$, we have a bijection between $Y_H(K)$ and the set of elliptic curves over $K$ with $H$-structure. Note that Equation (1.1), for fields with characteristic $p \nmid n$, means that $(E, \phi) \sim_H (E', \phi')$ if and only if the matrix associated to the action of $\iota|_{E[n]}$ relatively to the $\mathbb{Z}/n\mathbb{Z}$-bases of $E[n]$ and $E'[n]$ defined via $\phi$ and $\phi'$, respectively, belongs to $H$.

*Remark* 1.2. Since $-1$ is an automorphism of every elliptic curve, then for every $H$, the curve $X_H$ is isomorphic to $X_{\pm H}$, where $\pm H := \{\pm \mathrm{Id}\}{\cdot}H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Hence, the equivalence relation (1.1) can be written as follows

$$(E,\phi) \sim_H (E',\phi') \iff (\phi')^{-1} \circ \iota|_{E[n]} \circ \phi = h, \text{ for some } h \in \pm H \text{ and } \iota\colon E \xrightarrow{\sim} E'.$$

Let $\mathbb{H}$ be the complex upper half-plane $\{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$, let $\mathbb{H}^{\pm} = \mathbb{C} - \mathbb{R}$ and moreover let $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ and $\overline{\mathbb{H}}^{\pm} = \mathbb{H}^{\pm} \cup \mathbb{P}^1(\mathbb{Q})$ be their "compactifications". The group $\mathrm{GL}_2(\mathbb{Z})$ acts on $\mathbb{H}^{\pm}$ and $\overline{\mathbb{H}}^{\pm}$ by Möbius transformations. Moreover, every $g$ in $\mathrm{GL}_2(\mathbb{Z})$ acts on pairs $(z, \gamma H) \in \mathbb{H}^{\pm} \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)$ as $(g(z), \bar{g}^{-T}\gamma H)$, where $g(z)$ is the image of $z$ under the Möbius transformation given by $g$ and $\bar{g}^{-T}$ is the transpose of the inverse of the reduction $\bar{g}$ of $g \bmod n$. This action gives canonical isomorphisms of Riemann surfaces

$$\mathrm{GL}_2(\mathbb{Z})\backslash\big(\mathbb{H}^{\pm} \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)\big) \longrightarrow Y_H(\mathbb{C}), \tag{1.3}$$

$$\mathrm{GL}_2(\mathbb{Z})\backslash\big(\overline{\mathbb{H}}^{\pm} \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)\big) \longrightarrow X_H(\mathbb{C}). \tag{1.4}$$

The isomorphism (1.3) is equivalent to that one described in [DR73, IV.5.3] and is given by $\mathrm{GL}_2(\mathbb{Z})(\tau, \gamma H) \mapsto (E_\tau, \phi_\tau \circ \gamma)$, where $E_\tau$ is the elliptic curve $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ and $\phi_\tau\colon (\mathbb{Z}/n\mathbb{Z})^2_{\mathbb{C}} \to E_\tau[n]$ is the unique isomorphism such that

$$\phi_\tau \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{\tau}{n}, \quad \phi_\tau \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{n}.$$

We notice that for each $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ and for each $\gamma \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, the two pairs $(E_\tau, \phi_\tau \circ \gamma)$ and $(E_{g(\tau)}, \phi_{g(\tau)} \circ \bar{g}^{-T}\gamma)$ are equivalent because the map $z \mapsto (c\tau + d)z$ gives an isomorphism $\iota\colon E_{g(\tau)} \to E_\tau$ such that $\phi_\tau^{-1} \circ \iota \circ \phi_{g(\tau)} = \bar{g}^T$. Consequently, we obtain an action of $\mathrm{GL}_2(\mathbb{Z})$ on pairs $(E_\tau, \phi_\tau \circ \gamma)$ which is the same as the action of Equation (1.3) and Equation (1.4). We notice that the transposition is necessary to make all the maps and the actions compatible.

The isomorphism (1.4) is just the extension of the previous one to the compactifications. For each subgroup $H$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we define

$$\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma^T \pmod{n} \text{ lies in } H\}.$$

If $\det H \neq (\mathbb{Z}/n\mathbb{Z})^\times$, then $X_H(\mathbb{C})$ is not connected: the number of connected components is $[(\mathbb{Z}/n\mathbb{Z})^\times : \det(H)]$ and, for each connected component $X_H^{cc}(\mathbb{C})$, there are isomorphisms of Riemann surfaces

$$\begin{aligned} \Gamma_{gHg^{-1}}\backslash\overline{\mathbb{H}} \longrightarrow X_H^{cc}(\mathbb{C}), \quad \Gamma_{gHg^{-1}}\backslash\mathbb{H} &\longrightarrow Y_H^{cc}(\mathbb{C}), \\ \Gamma_{gHg^{-1}}\tau &\mapsto (E_\tau, \phi_\tau \circ g), \end{aligned} \tag{1.5}$$

for some $g$ in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. In particular, if $\det H = (\mathbb{Z}/n\mathbb{Z})^\times$, then $Y_H$ and $X_H$ are geometrically connected curves defined over $\mathbb{Q}$.

The following proposition about the isomorphism (1.3) is used in Section 5.

**Proposition 1.6.** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let $g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and consider the composition*

$$\begin{tikzcd} \mathbb{H} \arrow[r] \arrow[rr, bend right] & \Gamma_{gHg^{-1}}\backslash\mathbb{H} \arrow[r, hook] & Y_H(\mathbb{C}), \end{tikzcd}$$

*where the left map is the natural projection and the right map is in (1.5). Then a point $(E, \phi) \in Y_H(\mathbb{C})$ is a branch point for such composition if and only if there is a non-trivial* *automorphism $u$ of $E$ such that $\phi^{-1}\circ u|_{E[n]}\circ\phi \in \pm H$. If this happens, then each point $\tau \in \mathbb{H}$ projecting to $(E,\phi)$ has ramification index* $\#\mathrm{Aut}(E)/2$.

*Proof.* By Remark 1.2 we can suppose that $H$ contains $-\mathrm{Id}$. Instead of looking at a map $\mathbb{H} \to Y_H(\mathbb{C})$ parametrizing a single component of $Y_H$, we can work with the canonical map

$$\begin{tikzcd} \mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \arrow[r, "\pi"] \arrow[rr, bend right] & Y(n)(\mathbb{C}) \arrow[r, "\pi_H"] & Y_H(\mathbb{C}). \end{tikzcd}$$

Up to substituting $n$ with $3n$ and $H$ with its preimage under $\mathrm{GL}_2(\mathbb{Z}/3n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we can suppose that $n \geqslant 3$. This implies that $\pi$ is an (unramified) covering map, hence the ramification index of the $\pi_H \circ \pi$ in a point $(\tau,\gamma)$ is equal to the ramification index of $\pi_H$ in the point $\pi(\tau,\gamma)$. Hence, we only need to look at the ramification points of $\pi_H$. A point $(E,\phi) \in Y_H(\mathbb{C})$ is a branch point for $\pi_H$ if and only if the fiber $\pi_H^{-1}(E,\phi)$ has cardinality smaller than $\deg \pi_H = \#H/2$. The modular interpretation of $Y_H$ and $Y(n)$ implies that

$$\pi_H^{-1}(E,\phi) = \big\{(E, u|_{E[n]}\circ\phi\circ h) : h \in H, u \in \mathrm{Aut}(E)\big\}/\mathrm{Aut}(E), \tag{1.7}$$

where $v \in \mathrm{Aut}(E)$ acts sending $(E,\psi)$ to $(E, v|_{E[n]}\circ\psi)$. Since $n \geqslant 3$, the map that sends $u$ to $\phi^{-1}\circ u|_{E[n]}\circ\phi$ gives an inclusion $\mathrm{Aut}(E) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, hence, by (1.7), we have

$$\#\pi_H^{-1}(E,\phi) = \#\Big((H\cdot\mathrm{Aut}(E))/\mathrm{Aut}(E)\Big) = \#\Big(H/(H\cap\mathrm{Aut}(E))\Big).$$

The group $\mathrm{Aut}(E)$ always contains the multiplication by $-1$ and is cyclic of order $2, 4$ or $6$. Finally, there are two options for $\mathrm{Aut}(E)\cap H$:

- $\mathrm{Aut}(E)\cap H$ only contains $\pm\mathrm{Id}$ and $(E,\phi)$ is not a branch point;
- $\mathrm{Aut}(E)\cap H$ has order equal to $\#\mathrm{Aut}(E) > 2$, in this case $(E,\phi)$ is a branch point and, since the map $\pi_H$ is Galois, every point in $\pi_H^{-1}(E,\phi)$ has ramification index $\deg(\pi_H)/\#\pi_H^{-1}(E,\phi) = \#\mathrm{Aut}(E)/2$.

□

*Remark* 1.8. Notice that all the statements of Section 1 and Section 2 are presented for a subgroup $H$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, which is not defined for $n = 1$. However, we can deduce all the same conclusions for the curve $X(1)$ since it is isomorphic to $X_H$ with, for example, $n = 3$ and $H = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (in this case, of course $n$ is not the level of the modular curve in the usual sense).

## 2. Hecke operators

Let $n$ be a positive integer and let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For every prime $\ell \nmid n$, there is a divisor $D_\ell \subset X_H \times X_H$ inducing the $\ell$-th Hecke operator

$$T_\ell \colon \mathrm{Div}(X_H) \to \mathrm{Div}(X_H), \quad T_\ell \colon \mathrm{Jac}(X_H) \to \mathrm{Jac}(X_H).$$

On $Y_H(\mathbb{C})$, it is described by

$$T_\ell(E,\phi) = \sum_{0 \lneq C \lneq E[\ell]} (E/C, \pi_C \circ \phi), \tag{2.1}$$

where $\pi_C \colon E \to E/C$ is the natural projection. Now we recall the definition of $T_\ell$. Let $H_\ell$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\ell\mathbb{Z})$ containing the matrices whose reduction modulo $n$ lies in $H$ and whose reduction modulo $\ell$ is an upper triangular matrix. Given a $\mathbb{Z}[\frac{1}{n\ell}]$-scheme $S$ and an elliptic curve $E/S$ with $H_\ell$-structure $\phi\colon (\mathbb{Z}/n\ell\mathbb{Z})^2 \to E[n\ell]$, we have two ways of constructing an elliptic curve over $S$ with $H$-structure:

- The $n$-torsion subgroup of $(\mathbb{Z}/n\ell\mathbb{Z})^2$ is canonically isomorphic, via the Chinese Remainder Theorem, to $(\mathbb{Z}/n\mathbb{Z})^2$ and the restriction of $\phi$ to this subgroup gives an isomorphism $\phi|_{(\mathbb{Z}/n\mathbb{Z})^2}\colon (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$. One can check that the class of $(E, \phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$ modulo $\sim_H$ does not depend on the choice of the representative $(E,\phi)$ in the equivalence class defined by $\sim_{H_\ell}$, hence
$$\mathrm{pr}(E,\phi) := (E, \phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$$
is a well defined elliptic curve over $S$ with $H$-structure.
- The subgroup $C \subset E[\ell]$ generated by $\phi(\begin{smallmatrix} n \\ 0 \end{smallmatrix})$ is a subgroup of $E$ of order $\ell$ and $E/C$ is an elliptic curve over $S$. Denoting by $\pi_C\colon E \to E/C$ the natural projection, we have that
$$\mathrm{qt}(E,\phi) := (E/C, \pi_C \circ \phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$$
is a well defined elliptic curve over $S$ with $H$-structure.

These two constructions define natural transformations between the functor of elliptic curves with $H_\ell$-structure and the functor of elliptic curves with $H$-structure restricted to schemes over $\mathbb{Z}[\frac{1}{n\ell}]$. We get induced morphisms between the coarse moduli spaces $Y_{H_\ell}$ and $(Y_H)_{\mathbb{Z}[\frac{1}{n\ell}]}$ that can be extended by smoothness to the compactifications:
$$\mathrm{pr}, \mathrm{qt}\colon X_{H_\ell} \longrightarrow (X_H)_{\mathbb{Z}[\frac{1}{n\ell}]}.$$
The image of $X_{H_\ell}$ under the map $(\mathrm{pr}, \mathrm{qt})$ defines a divisor inside $(X_H)_{\mathbb{Z}[\frac{1}{n\ell}]} \times (X_H)_{\mathbb{Z}[\frac{1}{n\ell}]}$. Since $X_H$ is smooth over $\mathbb{Z}[\frac{1}{n}]$, this divisor extends uniquely to $D_\ell \subset X_H \times X_H$ whose irreducible components project surjectively on each factor $X_H$. This correspondence induces the operator $T_\ell = \mathrm{qt}_* \circ \mathrm{pr}^*$ and the definitions of qt and pr imply the equality (2.1).

The reduction of $T_\ell$ modulo $\ell$ is described by a celebrated theorem of Eichler and Shimura. To state this theorem in the full generality, we recall the definition of diamond operators. Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, then the matrix $(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix})$ normalizes $H$, hence
$$\langle a \rangle (E,\phi) := (E, \phi \circ (\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}))$$
defines an automorphism of the functor of elliptic curves with $H$-structure. So $\langle a \rangle$ induces an automorphism of the coarse moduli space $Y_H$ and it extends to an automorphism of the compactification $X_H$. Eichler-Shimura Relation is nowadays a common knowledge, but in the literature is often stated in a different form than we need. The proof of [DS05, Theorem 8.7.2] can be directly adapted to our case, and another proof is in [Shi71a, Theorem 7.9 and Corollary 7.10]. We use the result in the following form.

**Theorem (Eichler-Shimura Relation).** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let $\ell$ be a prime number not dividing $n$, let $\overline{X}_H$ be the reduction of $X_H$ modulo $\ell$, let $\overline{T}_\ell, \overline{\langle \ell \rangle}\colon \mathrm{Div}(\overline{X}_H) \to \mathrm{Div}(\overline{X}_H)$ be the reduction of the Hecke operator $T_\ell$ and of the diamond operator $\langle \ell \rangle$ and let $\mathrm{Frob}_\ell\colon \overline{X}_H \to \overline{X}_H$ be the Frobenius morphism. Then*
$$\overline{T}_\ell = (\mathrm{Frob}_\ell)_* + \overline{\langle \ell \rangle}_* \circ (\mathrm{Frob}_\ell)^*.$$

Notice that in general $X_H$ is not geometrically connected and if $X'$ is a connected component of $\overline{X}_H$, the Frobenius morphism $\overline{X}_H \to \overline{X}_H$ may not restrict to a morphism $X' \to X'$. Analogously, if $x$ is a point on $X'$, the divisor $T_\ell(x)$ may be not supported on $X'$. We are interested in Eichler-Shimura Relation because, as already pointed out in [KM88, Lemma 2.6], it implies that, in certain cases, the automorphisms of modular curves automatically commute with all Hecke operators $T_\ell$.

**Proposition 2.2.** *Let $n$ be a positive integer, let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a subgroup containing the scalar matrices and such that $\det H = (\mathbb{Z}/n\mathbb{Z})^\times$. Let $\ell$ be a prime not dividing $n$ and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at $\ell$. Then, for any automorphism $u$ of $X_H$ defined over a compositum of quadratic fields, in $\mathrm{End}(\mathrm{Jac}(X_H))$ we have*

$$T_\ell \circ u = u^\sigma \circ T_\ell, \tag{2.3}$$

*where we identify $u$ and $u^\sigma$ with their pushforward on $\mathrm{Jac}(X_H)$. Moreover, if the gonality of $X_H(\mathbb{C})$ is greater than $2(\ell+1)$, then (2.3) holds at level of divisors.*

*Proof.* Let $J := \mathrm{Jac}(X_H)$, let $\mathrm{Frob}_\ell \colon \overline{X}_H \to \overline{X}_H$ be the Frobenius morphism and let $\phi_\ell$ be the Frobenius generator of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. Let $D \in \mathrm{Div}(\overline{X}_H)$ and let $\bar{u}$ be the reduction of $u$ modulo $\ell$. Using Eichler-Shimura Relation, we have

$$\begin{aligned}\overline{T}_\ell \circ \bar{u}(D) &= ((\mathrm{Frob}_\ell)_* + (\mathrm{Frob}_\ell)^*) \circ \bar{u}(D) = (\mathrm{Frob}_\ell)_* \bar{u}(D) + (\mathrm{Frob}_\ell)^* \bar{u}(D) = \\ &= \bar{u}^{\phi_\ell}(\mathrm{Frob}_\ell)_*(D) + \bar{u}^{\phi_\ell^{-1}}(\mathrm{Frob}_\ell)^*(D) = \overline{u^\sigma}(\mathrm{Frob}_\ell)_*(D) + \overline{u^{\sigma^{-1}}}(\mathrm{Frob}_\ell)^*(D).\end{aligned}$$

Now, since $u$ is defined over a compositum of quadratic fields, the Galois automorphisms $\sigma$ and $\sigma^{-1}$ act in the same way on $u$. This implies that the last term in the previous chain of equalities is equal to $\overline{u^\sigma} \circ \overline{T}_\ell(D)$ obtaining $\overline{T}_\ell \circ \bar{u} = \overline{u^\sigma} \circ \overline{T}_\ell$ in $\mathrm{End}(J_{\mathbb{F}_\ell})$.

Since $J$ has good reduction at $\ell$, the natural map $\mathrm{End}(J) \to \mathrm{End}(J_{\mathbb{F}_\ell})$ is injective, hence (2.3) holds in $\mathrm{End}(J)$. This means that, for any two points $P$ and $Q$ in $X_H(\mathbb{C})$, the divisor $D := (T_\ell u - u^\sigma T_\ell)(P - Q)$ is principal. Hence, either $D$ is the zero divisor or is the divisor of a non-constant rational function on $X_H$ of degree at most $2(\ell+1)$.

Now we suppose that the gonality of $X_H$ exceeds $2(\ell+1)$. In this case, there are no non-constant rational functions on $X_H$ of degree at most $2(\ell+1)$, hence $D$ is the zero divisor. This gives the following equality of divisors:

$$T_\ell u(P) + u^\sigma T_\ell(Q) = u^\sigma T_\ell(P) + T_\ell u(Q).$$

For every point $P$, we can choose $Q$ such that the supports of $T_\ell u(P)$ and $T_\ell u(Q)$ are disjoint, and, therefore, last equality implies $T_\ell u(P) = u^\sigma T_\ell(P)$ as divisors. Up to a base change to $\mathbb{C}$, each divisor on $X_H$ is a sum of points with integer coefficients, hence we conclude that (2.3) holds at level of divisors. □

**Multiple points in the image of Hecke operators.** In the proofs of Section 5 we look at points $P \in X_H(\mathbb{C})$ and primes $\ell$ such that $T_\ell(P)$ is not a sum of distinct points. In this subsection we study this phenomenon. We denote by $\rho = e^{\frac{2\pi i}{3}}$ the primitive third root of unity contained in $\mathbb{H}$. Moreover, for every $\tau \in \mathbb{H}$, we denote by $E_\tau$ the elliptic curve $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. The main result is the following

**Theorem 2.4.** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let $\ell \geqslant 5$ be a prime not dividing $n$. Then, for all points $P \in X_H(\mathbb{C})$, we have that:*

1. *in $T_\ell(P)$ there is a point with multiplicity at least 4 if and only if $P$ is a cusp;*
2. *in $T_\ell(P)$ there is a point with multiplicity 3 if and only if $P = (E_\rho, \phi)$ for some $\phi$ such that and the matrix $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi$ lies in $\pm H$;*
3. *in $T_\ell(P)$ there are two distinct points with multiplicity 2 if and only if $P = (E_i, \phi)$ for some $\phi$ such that the matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$.*

*Proof.* This immediately follows from the following Propositions 2.5, 2.7 and 2.9. □

When $P$ is a cusp, we have the following result.

**Proposition 2.5.** *Let $n$ be a positive integer and let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let $\ell$ be a prime number not dividing $n$, let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at $\ell$ and let $C \in X_H(\overline{\mathbb{Q}})$ be a cusp. Then, at the level of divisors we have*

$$T_\ell(C) = C^\sigma + \ell\langle\ell\rangle(C^{\sigma^{-1}}).$$

*Proof.* The divisor $T_\ell(C) = \mathrm{qt}_*\mathrm{pr}^*(C)$ is supported on the cusps because the maps $\mathrm{pr}, \mathrm{qt}\colon X_{H_\ell} \to X_H$ send non-cuspidal points to non-cuspidal points and cusps to cusps. If we fix a prime ideal $\mathfrak{l}$ in the algebraic integers such that $\mathfrak{l} \mid \ell$, then, by [DR73, IV.3.4], each cusp in $X_H(\overline{\mathbb{Q}})$ reduces to a different point modulo $\mathfrak{l}$. Thus, it is enough to prove that $T_\ell(C)$ is congruent to $C^\sigma + \ell\langle\ell\rangle(C^{\sigma^{-1}})$ modulo $\mathfrak{l}$, and this is true by Eichler-Shimura Relation. □

We need a criterion to characterize the points $(E, \phi) \in Y_H(\mathbb{C})$ such that their image via $T_\ell$ contains a point with multiplicity at least 2. It is given by the following lemma.

**Lemma 2.6.** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let $\ell$ be a prime not dividing $n$. For all points $(E, \phi), (E', \phi') \in Y_H(\mathbb{C})$ and all positive integers $m \geqslant 2$, the following are equivalent:*

1. *$T_\ell(E, \phi)$ contains $(E', \phi')$ with multiplicity $m$;*
2. *there are $m$ isogenies $\alpha_1, \dots, \alpha_m\colon E \to E'$ of degree $\ell$ with distinct kernels such that $(\phi')^{-1} \circ \alpha_j|_{E[n]} \circ \phi$ lies in $\pm H$, for every $j = 1, \dots, m$;*
3. *there are $m$ endomorphisms $\beta_1 = \ell, \beta_2, \dots, \beta_m$ of $E'$ of degree $\ell^2$ and an isogeny $\alpha\colon E' \to E$ of degree $\ell$ such that:*

**P1:** *$\beta_i \neq u \circ \beta_j$, for $i, j = 1, \dots, m$, such that $i \neq j$ and for each $u \in \mathrm{Aut}(E')$;*
**P2:** *$\ker \alpha \subset \ker \beta_j$, for every $j = 1, \dots, m$;*
**P3:** *the matrices $\ell^{-1}\phi^{-1} \circ \alpha|_{E'[n]} \circ \phi'$ and $\ell^{-1}(\phi')^{-1} \circ \beta_j|_{E'[n]} \circ \phi'$ lie in $\pm H$, for every $j = 1, \dots, m$, where $\ell^{-1}$ is the inverse of the scalar matrix $\ell \bmod n$.*

*Proof.* The equivalence between (1) and (2) follows by definition of Hecke operator. Now we prove the equivalence between (2) and (3). Let $\alpha_1, \dots, \alpha_m$ be isogenies of degree $\ell$ with distinct kernels, then it is enough to take $\alpha$ equal to the dual of $\alpha_1$ and $\beta_j = \alpha_j \circ \alpha$, for $j = 1, \dots, m$. Conversely, if $\beta_1, \dots, \beta_m$ respect the three properties above, then, for every $j = 1, \dots, m$, we can take $\alpha_j$ to be the unique isogeny such that $\beta_j = \alpha_j \circ \alpha$. □

In the next two propositions we study some cases in which $T_\ell(E, \phi)$ contains points with higher multiplicity, with a particular attention to $E_i$ and $E_\rho$. Namely, Proposition 2.9 characterizes when $\phi^{-1} \circ \tau|_{E_\tau[n]} \circ \phi$ belongs to $\pm H$, for $\tau = \rho, i$, in terms of the multiplicities shown in the divisor $T_\ell(E_\tau, \phi)$, while Proposition 2.7 proves that if $T_\ell(E, \phi)$ shows certain multiplicities, then $E$ has complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\rho)$.

**Proposition 2.7.** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let $\ell$ be a prime not dividing $n$ and let $(E, \phi)$ be a $\mathbb{C}$-point of $Y_H$. Then:*

1. *the points in the image $T_\ell(E, \phi)$ have multiplicity at most 3;*
2. *if $T_\ell(E, \phi)$ contains a point with multiplicity 3, then $E \cong E_\rho$;*
3. *if there are two distinct points of $Y_H(\mathbb{C})$ appearing with multiplicity 2 in $T_\ell(E, \phi)$, then $E \cong E_i$.*

*Proof.* Parts (1) and (2).

First we prove that if $T_\ell(E,\phi)$ contains a point with multiplicity *at least* 3, then $E \cong E_\rho$. Let $(E',\phi') \in Y_H(\mathbb{C})$ be such that $T_\ell(E,\phi)$ contains $(E',\phi')$ with multiplicity at least 3. Lemma 2.6 implies the existence of isogenies $\alpha_1,\alpha_2,\alpha_3\colon E \to E'$ of degree $\ell$ with different kernels. For each $j \neq k$, we define $\gamma_{j,k} := \hat{\alpha}_j \circ \alpha_k \in \mathrm{End}(E)$, where $\hat{\alpha}_j$ is the dual of $\alpha_j$. Since $\alpha_k \neq \pm\alpha_j$, for all $j \neq k$, then

$$\gamma_{j,k} = \hat{\alpha}_j \circ \alpha_k \neq \pm\hat{\alpha}_j \circ \alpha_j = \pm\ell \in \mathrm{End}(E), \tag{2.8}$$

so $\gamma_{j,k}$ is cyclic of degree $\ell^2$. In particular $E$ has more than 2 endomorphisms of degree $\ell^2$, hence it has complex multiplication over some imaginary quadratic field $K$. We suppose by contradiction that $\mathrm{Aut}(E) = \{\pm 1\}$. In this case Equation (2.8) implies that $\ker(\gamma_{j,k}) \neq \ker(\ell) = E[\ell]$ and consequently that $\ker(\gamma_{j,k}) \cap E[\ell]$ has order $\ell$. Hence, for all $j \neq k$, we have that $\ker(\gamma_{j,k}) \cap E[\ell] = \ker(\alpha_k)$. In particular, the 12 endomorphisms $\pm\gamma_{j,k}$, with $j \neq k$, are pairwise distinct: if we had $\hat{\alpha}_j \circ \alpha_k = \pm\hat{\alpha}_r \circ \alpha_m$, then

$$\ker(\alpha_k) = \ker(\hat{\alpha}_j \circ \alpha_k) \cap E[\ell] = \ker(\hat{\alpha}_r \circ \alpha_m) \cap E[\ell] = \ker(\alpha_m),$$

implying $k = m$ and, consequently, $j = r$. Let $\mathcal{O}_K$ be the ring of integers of $K$ and let $m$ be the unique positive integer such that $\mathrm{End}(E) = \mathbb{Z} + m\mathcal{O}_K$. If $\ell \mid m$, the only elements of $\mathbb{Z} + m\mathcal{O}_K$ having norm divisible by $\ell$ belong to $\ell\mathcal{O}_K$, hence all the elements of $\mathrm{End}(E)$ having degree $\ell^2$ have form $\ell u$, for $u \in \mathcal{O}_K^\times$. Hence there are at most 6 of such elements. If $\ell \nmid m$, the ideals of norm $\ell^2$ inside $\mathrm{End}(E)$ are in bijection with the ideals of norm $\ell^2$ inside $\mathcal{O}_K$. Hence, by looking at the possible factorizations, there are at most 3 of such ideals and therefore at most 6 elements of $\mathrm{End}(E)$ of degree $\ell^2$. In all the cases there are at most 6 elements of $\mathrm{End}(E)$ of degree $\ell^2$, implying that the elements $\pm\gamma_{j,k}$ are not distinct, which is a contradiction.

We excluded the cases where $\mathrm{Aut}(E) = \{\pm 1\}$, it remains to exclude the case $E \cong E_i$. We suppose $E \cong E_i$ and we look at $\delta_k := \gamma_{k,3}$, for $k = 1, 2$. Since $\pm\delta_2, \pm\delta_1, \pm\ell$ are distinct, then at least one of the $\delta_k$'s is not contained in $\{\pm\ell, \pm i\ell\}$ and, up to renaming, we can suppose that this happens for $\delta_2$. Hence, we can factor $\delta_2 = i^r\lambda^2$, for some integer $r$ and some prime element $\lambda \in \mathbb{Z}[i] = \mathrm{End}(E)$. We deduce that $\ker(\alpha_3) = \ker(\delta_2) \cap E[\ell] = \ker(\lambda)$ and consequently

$$E' \cong E/\ker(\alpha_3) = E/\ker(\lambda) \cong E_i.$$

Up to units of $\mathrm{End}(E)$, there are at most 2 elements of $\mathrm{End}(E) \cong \mathrm{Hom}(E,E')$ of degree $\ell$, contradicting the existence of $\alpha_1,\alpha_2,\alpha_3$ and proving that $E \cong E_\rho$.

Finally, we prove that $T_\ell(E,\phi)$ does not contain points with multiplicity greater than 3. We suppose by contradiction that $T_\ell(E,\phi)$ contains $(E',\phi')$ with multiplicity at least 4. Because of the previous step, we have $E \cong E_\rho$. Since, up to unit, there are at most 2 elements of $\mathrm{End}(E_\rho)$ of degree $\ell$, then there are at most 2 points of $T_\ell(E_\rho,\phi)$ of the form $(E_\rho,\varphi)$ and consequently $E' \ncong E_\rho$ which is equivalent to $\mathrm{End}(E') \neq \mathbb{Z}[\rho]$. The isogenies between $E$ and $E'$ give an inclusion $\ell\mathrm{End}(E) \subset \mathrm{End}(E')$, implying that $\mathrm{End}(E') = \mathbb{Z}[\ell\rho]$. Hence the only elements in $\mathrm{End}(E')$ of degree $\ell^2$ are $\pm\ell, \pm\rho\ell, \pm\rho^2\ell$, contradicting the existence of $\beta_1,\beta_2,\beta_3,\beta_4$ as in Lemma 2.6, Condition (3). This contradiction concludes the proof of Parts (1) and (2).

Part (3).

Let $(E',\phi'), (E'',\phi'') \in Y_H(\mathbb{C})$ be such that $T_\ell(E,\phi) = 2(E',\phi') + 2(E'',\phi'') + D$ where the support of $D$ does not contain neither $(E',\phi')$ nor $(E'',\phi'')$. By Lemma 2.6 there are isogenies $\alpha_1,\alpha_2\colon E \to E'$ and isogenies $\alpha_3,\alpha_4\colon E \to E''$ such that the subgroups

$\ker(\alpha_i)$, for $i = 1, \dots, 4$, are four different subgroups of $E[\ell]$ of order $\ell$. By looking at the endomorphisms $\gamma_{j,k} := \hat{\alpha}_j \circ \alpha_k \in \mathrm{End}(E)$ for $(j,k) \in \{(1,2),(2,1),(3,4),(4,3)\}$, we can exclude the case $\mathrm{Aut}(E) = \{\pm 1\}$ with the same arguments used for Parts (1) and (2). To prove Part (3) it remains to exclude the case $E \cong E_\rho$. We suppose by contradiction $E \cong E_\rho$. Since, up to unit, there are at most 2 elements of $\mathrm{End}(E_\rho)$ of degree $\ell$, then there are at most 2 points of $T_\ell(E_\rho, \phi)$ of the form $(E_\rho, \varphi)$. Hence we can suppose $E' \not\cong E_\rho$ which, as in the proof of Parts (1) and (2), implies $\mathrm{End}(E') = \mathbb{Z}[\ell\rho]$. By Lemma 2.6, there are $\alpha$, $\beta_1 = \ell$ and $\beta_2$ satisfying **P1**, **P2**, **P3** of Lemma 2.6. In $\mathbb{Z}[\ell\rho]$ the only elements of norm $\ell^2$ have form $\rho^k\ell$, hence $\beta_2$ has the same form for some $k \in \{1,2,4,5\}$. We define $\beta_3 := \rho^{2k}\ell = \ell^{-1}\beta_2^2$ that satisfies property **P3** of Lemma 2.6 and, since $\mathrm{End}(E') = \mathbb{Z}[\ell\rho]$, the elements $\beta_1, \beta_2, \beta_3$ satisfy the property **P1**. We now prove that $\beta_3$ satisfies property **P2** as well. Since $\ker(\alpha) \subset \ker(\beta_2)$, we can write $\beta_2 = \gamma \circ \alpha$ for some isogeny $\gamma\colon E_\rho \to E'$ of degree $\ell$. Notice that, if $\alpha \circ \gamma \in \mathrm{End}(E_\rho)$ was not a multiple of $\ell$, then we would have $\alpha \circ \gamma = u\lambda^2$, for some $u \in \mathrm{Aut}(E_\rho)$ and some element $\lambda \in \mathrm{End}(E_\rho)$ of degree $\ell$, implying

$$\ker(\lambda) = \ker(u\lambda^2) \cap E_\rho[\ell] \supset \ker(\gamma).$$

Since $\ker(\lambda)$ and $\ker(\gamma)$ have the same cardinality, this implies that $\ker(\lambda) = \ker(\gamma)$, and therefore that $E_\rho \cong E_\rho/\ker(\lambda) = E_\rho/\ker(\gamma) \cong E'$, which is absurd. We deduce that $\alpha \circ \gamma = \ell\delta$ for some $\delta \in \mathrm{End}(E_\rho)$, hence we can write

$$\beta_3 = \ell^{-1}\beta_2^2 = \gamma \circ \delta \circ \alpha \quad \Longrightarrow \quad \ker(\alpha) \subset \ker(\beta_3),$$

which is property **P2** of Lemma 2.6. Applying Lemma 2.6 once again, we deduce that $(E', \phi')$ appears in $T_\ell(E, \phi)$ with multiplicity 3, which is a contradiction. □

**Proposition 2.9.** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let $\ell$ be a prime not dividing $n$.*

*(1) Let $(E_\rho, \phi) \in Y_H(\mathbb{C})$. The matrix $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi$ lies in $\pm H$ if and only if the divisor $T_\ell(E_\rho, \phi)$ contains a point with multiplicity 3.*

*(2) Let $(E_i, \phi) \in Y_H(\mathbb{C})$. If $\ell > 2$: The matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$ if and only if there are two distinct points of $Y_H(\mathbb{C})$ appearing with multiplicity 2 in $T_\ell(E_i, \phi)$. If $\ell = 2$: The matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$ if and only if there are two distinct points $P_1, P_2 \in Y_H(\mathbb{C})$ such that $T_2(E_i, \phi) = 2P_1 + P_2$.*

*Proof.* Part (1).

If $C \subset E_\rho[\ell]$ is a subgroup of order $\ell$, then $\rho C$ and $\rho^2 C$ are subgroups of order $\ell$ as well and there are two unique isomorphisms $u, v$ that make the following diagrams commutative:

$$\begin{tikzcd} E_\rho \arrow[r, "\rho"] \arrow[d, "\pi_C"] & E_\rho, \arrow[d, "\pi_{\rho C}"] \\ E_\rho/C \arrow[r, "u"] & E_\rho/\rho C, \end{tikzcd} \qquad \begin{tikzcd} E_\rho \arrow[r, "\rho^2"] \arrow[d, "\pi_C"] & E_\rho \arrow[d, "\pi_{\rho^2 C}"] \\ E_\rho/C \arrow[r, "v"] & E_\rho/\rho^2 C. \end{tikzcd}$$

We have that $\rho C = C$ if and only if $\rho$ is an endomorphism of $E_\rho/C$, which is in turn equivalent to $\mathrm{Aut}(E_\rho/C) \neq \{\pm 1\}$ or $\mathrm{End}(E_\rho/C) = \mathbb{Z}[\rho]$ and, since the class number of $\mathbb{Z}[\rho]$ is equal to 1, this is equivalent to $E_\rho/C \cong E_\rho$. Hence, if $\rho C \neq C$, then $\mathrm{Aut}(E_\rho/C) = \{\pm 1\}$

and, using that $\pi_C$ and $\pi_{\rho C}$ are bijections on the $n$-torsion subgroups, we have

$$\begin{aligned}(E_\rho/C, \pi_C\circ\phi) = (E_\rho/\rho C, \pi_{\rho C}\circ\phi) &\iff (\pi_{\rho C}|_{E_\rho[n]}\circ\phi)^{-1}\circ u|_{(E_\rho/C)[n]}\circ(\pi_C|_{E_\rho[n]}\circ\phi) \in \pm H\\ &\iff \phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi \in \pm H.\end{aligned}\tag{2.10}$$

Analogously, $\rho^2 C \neq C$ if and only if $\operatorname{Aut}(E_\rho/C) = \{\pm 1\}$ and when this happens

$$(E_\rho/C, \pi_C\circ\phi) = (E_\rho/\rho^2 C, \pi_{\rho^2 C}\circ\phi) \quad\iff\quad \phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi \in \pm H.\tag{2.11}$$

The endomorphism $\rho$ does not act as a scalar on $E_\rho[\ell]$: if it acted as a scalar $k$, then $\rho - k = \ell a + \ell b\rho$, with $a, b \in \mathbb{Z}$, implying $\ell b = 1$ that is impossible. Hence, there are at most two non-trivial subgroups of $E_\rho[\ell]$ that are $\rho$-stable. In particular we can take a non-trivial subgroup $C_0$ such that $C_0$, $\rho C_0$ and $\rho^2 C_0$ are pairwise distinct.

If $\phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi$ lies in $\pm H$, then, by (2.10) and (2.11),

$$T_\ell(E_\rho, \phi) \geqslant (E_\rho/C_0, \pi_{C_0}\circ\phi) + (E_\rho/\rho C_0, \pi_{\rho C_0}\circ\phi) + (E_\rho/\rho^2 C_0, \pi_{\rho^2 C_0}\circ\phi) = 3(E_\rho/C_0, \pi_{C_0}\circ\phi).$$

Conversely, if $T_\ell(E_\rho, \phi)$ contains a point with multiplicity 3, there are three pairwise distinct subgroups $C_1, C_2, C_3 \subset E_\rho[\ell]$ of order $\ell$ such that

$$(E_\rho/C_1, \pi_{C_1}\circ\phi) = (E_\rho/C_2, \pi_{C_2}\circ\phi) = (E_\rho/C_3, \pi_{C_3}\circ\phi).$$

If one of the $C_j$ is $\rho$-stable, then $E_\rho/C_1 \cong E_\rho/C_2 \cong E_\rho/C_3 \cong E_\rho$, and $C_1, C_2, C_3$ are all $\rho$-stable, contradicting that there are at most two non-trivial $\rho$-stable subgroups of $E_\rho[\ell]$. In particular $\mathbb{Z}[\rho] \supsetneq \operatorname{End}(E_\rho/C_1)$ and since $E/C_1$ is $\ell$-isogenous to $E_\rho$ we deduce that $\operatorname{End}(E_\rho/C_1) = \mathbb{Z}[\ell\rho]$. Hence, the only endomorphisms of $E_\rho/C_1$ having degree $\ell^2$ are $\pm\ell, \pm\rho\ell, \pm\rho^2\ell$ and so there are at most three subgroups $C \subset E_\rho[\ell]$ of order $\ell$ such that $E_\rho/C$ is isomorphic to $E_\rho/C_1$, namely: $C_1, \rho C_1$ and $\rho^2 C_1$. We deduce that, up to reordering, $C_2 = \rho C_1$ hence, by (2.10), $\phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi$ lies in $\pm H$.

Part (2).

If $C \subset E_i[\ell]$ is a subgroup of order $\ell$, then $iC$ is a subgroup of order $\ell$ as well and there is a unique isomorphism $u$ that makes the following diagram commutative:

$$\begin{tikzcd} E_i \arrow[r, "i"] \arrow[d, "\pi_C"] & E_i \arrow[d, "\pi_{iC}"] \\ E_i/C \arrow[r, "u"] & E_i/iC. \end{tikzcd}$$

We have that $iC = C$ if and only if $\operatorname{End}(E_i/C) = \mathbb{Z}[i]$ if and only if $\operatorname{Aut}(E_i/C) \neq \{\pm 1\}$. Hence, if $iC \neq C$, then $\operatorname{Aut}(E_i/C) = \{\pm 1\}$ and, using that $\pi_C$ and $\pi_{iC}$ are bijections on the $n$-torsion subgroups, we have

$$\begin{aligned}(E_i/C, \pi_C\circ\phi) = (E_i/iC, \pi_{iC}\circ\phi) \quad&\iff\quad (\pi_{iC}\circ\phi)^{-1}\circ u|_{(E_i/C)[n]}\circ(\pi_C\circ\phi) \in \pm H\\ &\iff\quad \phi^{-1}\circ i|_{E_i[n]}\circ\phi \in \pm H.\end{aligned}\tag{2.12}$$

Similarly to the action of $\rho$ on $E_\rho[\ell]$, the endomorphism $i$ does not act as multiplication by a scalar on $E_i[\ell]$, hence there at most two non-trivial subgroups of $E_i[\ell]$ that are $i$-invariant. In other words, for each subgroup $C \subset E_i[\ell]$ of order $\ell$, except at most two, we have $C \neq iC$. If $\ell \geqslant 5$, since $T_\ell(E_i, \phi)$ contains $\ell+1 \geqslant 6$ points counted with multiplicity, we deduce the existence of $C_1, C_2$ such that $C_1, C_2, iC_1, iC_2$ are different cyclic subgroups of $E_i[\ell]$. When $\ell = 3$, the same conclusion is true because there is no subgroup of $E_i[3]$

which is invariant under the endomorphism $i$. If $\phi^{-1}\circ i|_{E_i[n]}\circ\phi$ lies in $\pm H$, then, by the equivalences (2.12), we have

$$\begin{aligned}T_\ell(E_i,\phi) \geqslant (E_i/C_1,\pi_{C_1}\circ\phi) + (E_i/iC_1,\pi_{iC_1}\circ\phi) + (E_i/C_2,\pi_{C_2}\circ\phi) + (E_i/iC_2,\pi_{iC_2}\circ\phi) =\\ = 2(E_i/C_1,\pi_{C_1}\circ\phi) + 2(E_i/C_2,\pi_{C_2}\circ\phi).\end{aligned}$$

Moreover $(E_i/C_1,\pi_{C_1}\circ\phi)$ and $(E_i/C_2,\pi_{C_2}\circ\phi)$ do not appear with multiplicity greater than 2 because of Proposition 2.7.

Now we assume that there are two distinct points $(E_i/C_1,\pi_{C_1}\circ\phi)$ and $(E_i/C_2,\pi_{C_2}\circ\phi)$ in $Y_H(\mathbb{C})$ appearing with multiplicity 2 in $T_\ell(E_i,\phi)$. Since there are at most two subgroups $C\subset E_i[\ell]$ such that $C=iC$, then there are at most two points, counted with multiplicity, in $T_\ell(E_i,\phi)$ having form $(E_i,\psi)$. Hence, up to reordering, we have $E_i/C_1\ncong E_i$, or equivalently $iC_1\neq C_1$. Thus $\mathrm{End}(E_i/C_1)=\mathbb{Z}[\ell i]$, and this implies that $\pm\ell$ and $\pm\ell i$ are the only elements of $\mathrm{End}(E_i/C_1)$ having degree $\ell^2$. Thus, applying Lemma 2.6 by checking Condition 3 on the modular curve $X(1)$ (see also Remark 1.8), we see that there is at most one cyclic subgroup $C\subset E_i[\ell]$ such that $E_i/C\cong E_i/C_1$ and $C\neq C_1$. Since $C=iC_1$ has this property and since $(E_i/C_1,\pi_{C_1}\circ\phi)$ appears in $T_\ell(E_i,\phi)$ with multiplicity 2, we have

$$(E_i/C_1,\pi_{C_1}\circ\phi) = (E_i/iC_1,\pi_{iC_1}\circ\phi),$$

and by the equivalences (2.12), we have that $\phi^{-1}\circ i|_{E_i[n]}\circ\phi$ lies in $\pm H$.

The case $\ell=2$ can be proven with similar arguments. □

## 3. Cartan modular curves and their jacobians

We give the definition of Cartan modular curves following [Ser97, Appendix A.5]. Let $n>1$ be an integer and let $A$ be a free commutative étale $\mathbb{Z}/n\mathbb{Z}$-algebra of rank 2. For each prime $p\mid n$, we have that $A/pA$ is isomorphic either to $\mathbb{F}_p\times\mathbb{F}_p$ or to $\mathbb{F}_{p^2}$: in the former we say that $A$ is *split* at $p$, in the latter we say that $A$ is *non-split* at $p$. Moreover, for every assignment of each prime $p|n$ to split or non-split, there is a unique, up to isomorphism, algebra $A$ which is split or non-split at every $p\mid n$ accordingly to the assignment.

We fix a $\mathbb{Z}/n\mathbb{Z}$-basis of $A$ and, consequently, we identify the automorphism group of $A$, as $\mathbb{Z}/n\mathbb{Z}$-module, with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The group $A^\times$ of the units of $A$ acts on $A$ by multiplication, giving an embedding of $A^\times$ inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. A subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which is the image of such an embedding is called a *Cartan subgroup*. The normalizer of $A^\times$ inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ contains all the matrices representing automorphisms of the ring $A$, hence $H:=\langle A^\times,\mathrm{Aut}_{\mathrm{Ring}}(A)\rangle$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ that contains $A^\times$ as normal subgroup. We call every such an $H$ a *Cartan-plus subgroup* of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The natural map $\mathrm{Aut}_{\mathrm{Ring}}(A)\to\prod_{p|n}\mathrm{Aut}_{\mathrm{Ring}}(A\otimes\mathbb{F}_p)$ is an isomorphism, hence $\mathrm{Aut}_{\mathrm{Ring}}(A)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(n)}$, where $\omega(n)$ is the number of prime divisors of $n$. In particular, given $A$, the Cartan subgroup has index $2^{\omega(n)}$ inside the Cartan-plus subgroup. Moreover, if $n$ is odd, the Cartan-plus is equal to the normalizer of the Cartan subgroup inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We call *Cartan modular curves* the modular curves associated to Cartan subgroups or to Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

When $n=p^e$ is a prime power, we use the following notation:

- $X_{\mathrm{ns}}^+(p^e):=X_H$, if $H$ is a Cartan-plus subgroup non-split at $p$;
- $X_{\mathrm{ns}}(p^e):=X_H$, if $H$ is a Cartan subgroup non-split at $p$;
- $X_{\mathrm{s}}^+(p^e):=X_H$, if $H$ is a Cartan-plus subgroup split at $p$;
- $X_{\mathrm{s}}(p^e):=X_H$, if $H$ is a Cartan subgroup split at $p$.

*Remark* 3.1. If $H_1$ and $H_2$ are two conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, then the corresponding modular curves $X_{H_1}$ and $X_{H_2}$ are isomorphic. Moreover, given two Cartan or two Cartan-plus subgroups $C_1$ and $C_2$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with the same assignment of each prime $p \mid n$ to split or non-split, then $C_1$ and $C_2$ are conjugate, so $X_{C_1} \cong X_{C_2}$. This implies that the above definitions are unambiguous.

*Remark* 3.2. Let $H_1$ and $H_2$ be subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\Gamma_{H_1} = g\Gamma_{H_2}g^{-1}$ for a suitable $g \in \mathrm{GL}_2(\mathbb{Q})$ with $\det(g) > 0$. In this case there is an isomorphism of Riemann surfaces given by

$$\begin{aligned} X_{H_1}(\mathbb{C}) &\to X_{H_2}(\mathbb{C}), \\ \Gamma_{H_1}\tau &\mapsto \Gamma_{H_2}g(\tau). \end{aligned}$$

See [DS05, Section 5.1] for more details about this.

We want to understand the structure, up to isogeny, of the jacobian of the Cartan modular curves. This is achieved using Chen's isogenies (see [Che98], [dSE00],[Che04]). Let $p$ be a prime and let $e$ be a positive integer. We give an analogous of [Che04, Theorem 1.1] involving the jacobian of $X_{\mathrm{ns}}(p^e)$ for every $p$, and, to do this, we extend the analysis in [Che04] to the case $p = 2$. In order to state our result, we choose a non-square element $\xi \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ when $p$ is odd and define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ for every prime $p$:

$$C_{\mathrm{s}}(p^e) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{s}}^+(p^e) := C_{\mathrm{s}}(p^e) \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{ns}}(2^e) := \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}^+(2^e) := C_{\mathrm{ns}}(2^e) \cup \left\{ \begin{pmatrix} a & a-b \\ b & -a \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}(p^e) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd};$$

$$C_{\mathrm{ns}}^+(p^e) := C_{\mathrm{ns}}(p^e) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd};$$

$$B_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^{r+1} & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, \quad ad \not\equiv 0 \bmod p \right\}, \quad \text{for } r = 0, 1, \ldots, e-1;$$

$$T_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^r & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, ad - bcp^{2r} \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\}, \quad \text{for } r = 0, 1, \ldots, e.$$

We remark that $T_e(p^e) = C_{\mathrm{s}}(p^e)$ and that $C_{\mathrm{s}}(p^e), C_{\mathrm{ns}}(p^e)$ are respectively a split and a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ and $C_{\mathrm{s}}^+(p^e), C_{\mathrm{ns}}^+(p^e)$ are the corresponding Cartan-plus subgroups.

**Proposition 3.3.** *Let $p$ be a prime, let $e$ be a positive integer and let $G = \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$. We have the following isomorphism of $\mathbb{Q}$-representations of $G$:*

$$\mathbb{Q}[G/C_{\mathrm{ns}}(p^e)] \oplus \bigoplus_{r=0}^{e-1} 2\mathbb{Q}[G/B_r(p^e)] \cong \mathbb{Q}[G/C_{\mathrm{s}}(p^e)] \oplus \bigoplus_{r=0}^{e-1} 2\mathbb{Q}[G/T_r(p^e)]. \tag{3.4}$$

*Proof.* We follow the same strategy of [Che04]. It is enough to prove that the representation on the right hand side has the same character of the representation on the left hand side. For every subgroup $H \subset G$, the character $\chi_H$ of the representation $\mathbb{Q}[G/H]$ is not hard to compute: for each $\gamma \in G$ we have $\gamma(gH) = (\gamma g)H$, hence, with respect to the basis $\{gH\}$, the matrix $M_\gamma$ associated to the action of $\gamma$ is a permutation matrix and consequently

$$\chi_H(\gamma) = \operatorname{tr}(M_\gamma) = \#\{gH : \gamma gH = gH\} = \frac{\#\{g : \gamma g \in gH\}}{\#H} = \frac{\#\{g : g^{-1}\gamma g \in H\}}{\#H}. \tag{3.5}$$

Hence to compute $\chi_H(\gamma)$ it is enough to compute $\#\{g : g^{-1}\gamma g \in H\}$ and $\#H$. It is enough to compute $\chi_H(\gamma)$ for a set of representatives $\gamma$ up to conjugation. We choose the same representatives as in [Che04, Table 2].

If $p = 2$, the character $\chi_H$ for the groups appearing in the statement is computed in the Appendix of this article. If $p$ is odd and $H$ has the form $B_r, T_r$ or $C_{\mathrm{s}}$, the character $\chi_H$ is given in [Che04, Tables 3 and 4]; if $p$ is odd and $H = C_{\mathrm{ns}}(p^e)$, then

$$\chi_H(g) = \begin{cases} (p-1)p^{2e-1}, & \text{if } g \text{ is a scalar matrix (type } I \text{ in [Che04, Tables 3, 4]),} \\ 2p^{2\mu}, & \text{if } g \text{ is a conjugate of } \left(\begin{smallmatrix} \alpha & \xi\beta p^\mu \\ \beta p^\mu & \alpha \end{smallmatrix}\right), \text{ with } \beta \in (\mathbb{Z}/p^e\mathbb{Z})^\times \\ & \text{ and } 0 \leqslant \mu < e-1 \text{ (types } RI'_\mu \text{ and } T' \text{ in [Che04, Tables 3, 4]),} \\ 0, & \text{otherwise.} \end{cases}$$

The characters of the representations in Equation (3.4) are sums of the previous characters. A straightforward computation proves the proposition. □

From the previous result about representations follows a result about jacobians of modular curves.

**Proposition 3.6.** *Let $p$ be a prime, let $e$ be a positive integer and let $J_{\mathrm{ns}}(p^e)$ be the jacobian of $X_{\mathrm{ns}}(p^e)$. We have the following isogenies over $\mathbb{Q}$:*

$$J_{\mathrm{ns}}(p^e) \times \prod_{r=0}^{e-1} J_0(p^{2r+1})^2 \sim J_0(p^{2e}) \times \prod_{r=0}^{e-1} J_0(p^{2r})^2, \qquad J_{\mathrm{ns}}(p^e) \sim \prod_{r=1}^{e} J_0^{\mathrm{new}}(p^{2r}).$$

*Proof.* For every $r = 0, \ldots, e-1$, let $w_{p^r} := \left(\begin{smallmatrix} 0 & -1 \\ p^r & 0 \end{smallmatrix}\right)$, then we have

$$w_{p^r}\Gamma_{B_r(p^e)}w_{p^r}^{-1} = \Gamma_0(p^{2r+1}) \qquad \text{and} \qquad w_{p^r}\Gamma_{T_r(p^e)}w_{p^r}^{-1} = \Gamma_0(p^{2r}),$$

that, by Remark 3.2, imply

$$X_0(p^{2r+1}) \cong X_{B_r(p^e)} \qquad \text{and} \qquad X_0(p^{2r}) \cong X_{T_r(p^e)} \tag{3.7}$$

respectively.

As explained in [dSE00, Théorème 2 and the discussion below it], the representation theoretic result in Proposition 3.3, together with the isomorphisms in Equation (3.7), implies the first isogeny. The argument to prove the second isogeny is the same, but we also need the isogeny $J_0(p^e) \sim \prod_{r=0}^{e} J_0^{\mathrm{new}}(p^r)^{\sigma_0(p^{e-r})}$, where $\sigma_0(m)$ is the number of positive divisors of the integer $m$. □

The analogous statement for $J_{\mathrm{ns}}^+(p^e)$ and $p$ odd is given in [Che04, Theorem 1.2]. For jacobians of Cartan curves of composite level we have the following theorem.

**Theorem 3.8.** *Let $n > 1$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a Cartan or a Cartan-plus subgroup. Then the jacobian of $X_H$ is a quotient of $J_0(n^2)$. More precisely, if $H$ is a Cartan subgroup, we have:*

$$\mathrm{Jac}(X_H) \sim \prod_{\substack{c\mid a^2\\ d\mid b}} J_0^{\mathrm{new}}(cd^2)^{\sigma_0\left(\frac{a^2}{c}\right)}, \tag{3.9}$$

*where $\sigma_0(m)$ is the number of positive divisors of an integer $m$ and $a, b$ are positive integers such that $n = ab$ and such that $H$ is split at all primes dividing $a$ and non-split at all primes dividing $b$.*

*Proof.* Since all the Cartan-plus subgroups contain a Cartan subgroup, we can suppose that $H$ is a Cartan subgroup. If $b = 1$, then $X_H(n) \cong X_0(n^2)$. Thus, we suppose that $b > 1$. Let $b = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of $b$ and for each $j = 1, \ldots, k$, we set $G_j := \mathrm{GL}_2(\mathbb{Z}/p_j^{e_j}\mathbb{Z})$ and $H_j := C_{\mathrm{ns}}(p_j^{e_j}) < G_j$. Moreover we set $G := \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and $G_{\mathrm{s}} := \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})$, and we choose a totally split Cartan subgroup $H_{\mathrm{s}} < G_{\mathrm{s}}$. Chinese Remainder Theorem gives an identification between $G$ and $G_{\mathrm{s}} \times \prod_{j=1}^k G_j$ sending $H$ to a conjugate of $H_s \times \prod_{j=1}^k H_j$.

Instead of working with $G$-representations up to isomorphism, it is easier to work inside the representation ring of $G$, namely the Grothendieck ring of the category of finite-dimensional $G$-representations, where we can take differences of representations. By Proposition 3.3 we have the following equality in the representation ring of $G_j$ over $\mathbb{Q}$:

$$\mathbb{Q}\big[G_j/H_j\big] = \mathbb{Q}\big[G_j/K_j(p_j^{2e_j})\big] + 2\sum_{i=0}^{2e_j-1}(-1)^i\mathbb{Q}\big[G_j/K_j(p_j^i)\big],$$

where $K_j(p_j^{2r}) := T_r(p_j^{e_j})$, for $r = 0, \ldots, e_j$, and $K_j(p_j^{2r+1}) := B_r(p_j^{e_j})$, for $r = 0, \ldots, e_j-1$. Interpreting $G_j$-representations as $G$-representations via the reduction modulo $p_j^{e_j}$ map, the above equality also holds in the representation ring of $G$ over $\mathbb{Q}$. We now get information about the representation $\mathbb{Q}[G/H]$ by taking the tensor product of the above identities, for $j = 1, \ldots, k$, and using that, for all the groups $\mathcal{G}_1, \mathcal{G}_2$ and all the subgroups $\mathcal{H}_i < \mathcal{G}_i$, we have the isomorphisms of $(\mathcal{G}_1\times\mathcal{G}_2)$-representations

$$\mathbb{Q}[\mathcal{G}_1/\mathcal{H}_1] \otimes \mathbb{Q}[\mathcal{G}_2/\mathcal{H}_2] \cong \mathbb{Q}[(\mathcal{G}_1\times\mathcal{G}_2)/(\mathcal{H}_1\times\mathcal{H}_2)].$$

Denoting by $\otimes$ the product in the representation ring of $G$ over $\mathbb{Q}$, we have

$$\begin{aligned}\mathbb{Q}\big[G/H\big] &= \mathbb{Q}\big[G_{\mathrm{s}}/H_s\big] \otimes \bigotimes_{j=1}^k \mathbb{Q}\big[G_j/H_j\big] = \\ &= \mathbb{Q}\big[G_{\mathrm{s}}/H_s\big] \otimes \bigotimes_{j=1}^k \left(\mathbb{Q}\big[G_j/K_j(p_j^{2e_j})\big] + 2\sum_{i=0}^{2e_j-1}(-1)^i\mathbb{Q}\big[G_j/K_j(p_j^i)\big]\right) = \\ &= \sum_{d\mid b^2} \varepsilon(d)m(d)\mathbb{Q}\big[G/K(d)\big],\end{aligned} \tag{3.10}$$

where, for every $d = p_1^{f_1} \cdots p_k^{f_k}$ dividing $b^2$, we have

$$\varepsilon(d) := (-1)^{f_1+\ldots+f_k}, \quad m(d) := 2^{\#\{j: f_j \neq 2e_j\}}, \quad K(d) := H_s \times \prod_{j=1}^k K_j(p_j^{f_j}) < G.$$

As explained in [dSE00], Equation (3.10) implies the following equality in the Grothendieck group of the category of abelian varieties over $\mathbb{Q}$ up to isogeny:

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} \mathrm{Jac}(X_{K(d)})^{\varepsilon(d)m(d)}.$$

Let

$$d_1 := \prod_{\substack{j=1 \\ f_j \text{ even}}}^{k} p_j^{\frac{f_j}{2}}, \quad d_2 := \prod_{\substack{j=1 \\ f_j \text{ odd}}}^{k} p_j^{\frac{f_j-1}{2}}, \quad p_o := \prod_{\substack{j=1 \\ f_j \text{ odd}}}^{k} p_j.$$

We have $d_1^2 d_2^2 p_o = d$ and the elements of $\Gamma_{K(d)}$ are exaclty those of the form $\left(\begin{smallmatrix} \alpha & \beta a d_1 d_2 p_o \\ \gamma a d_1 d_2 & \delta \end{smallmatrix}\right)$, with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ and $\alpha\delta - \beta\gamma a^2 d = 1$. Hence, $w_{ad_1d_2} \Gamma_{K(d)} w_{ad_1d_2}^{-1} = \Gamma_0(a^2 d)$, where $w_{ad_1d_2} := \left(\begin{smallmatrix} 0 & -1 \\ ad_1d_2 & 0 \end{smallmatrix}\right)$. By Remark 3.2, this gives an isomorphism $X_0(a^2d) \cong X_{K(d)}$ and consequently we have

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} J_0(a^2 d)^{\varepsilon(d)m(d)}.$$

Using $J_0(a^2d) \sim \prod_{m|a^2d} J_0^{\mathrm{new}}(m)^{\sigma_0\left(\frac{a^2d}{m}\right)}$ and the multiplicativity of the arithmetic functions $\varepsilon(d)$ and $m(d)$, one can compute that

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} J_0(a^2d)^{\varepsilon(d)m(d)} \sim \prod_{\substack{c|a^2 \\ d|b}} J_0^{\mathrm{new}}(cd^2)^{\sigma_0\left(\frac{a^2}{c}\right)}.$$

Hence, in the Grothendieck group of the category of abelian varieties over $\mathbb{Q}$ up to isogeny, $\mathrm{Jac}(X_H)$ is equal to an abelian subvariety of $J_0(n^2)$. This proves the theorem. □

*Remark* 3.11. In [Che04], Chen deals with Cartan curves and Cartan subroups whose level is an odd prime power. The computations in our Appendix allow us to extend Theorem 1.1 in [Che04], and therefore all the results contained in the paper, to the cases of level $2^e$, for $e$ a positive integer. Notice that $C_s^+(2^e)$ is different from the normalizer of $C_s(2^e)$, in fact at least $\left(\begin{smallmatrix} 1 & 2^{e-1} \\ 0 & 1 \end{smallmatrix}\right)$ always belongs to the normalizer but does not belong to $C_s^+(2^e)$. Substituting $C_s^+(p^e)$ with the normalizer of $C_s(p^e)$, Theorem 1.1 in [Che04] wouldn't extend to the case of level $2^e$.

Now we give a lower bound for the genus of Cartan modular curves: we show that for every $\varepsilon > 0$ the genus of a Cartan modular curve of level $n$ big enough is larger than $n^{2-\varepsilon}$.

**Proposition 3.12.** *Let $n \geqslant 10^5$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Denoting by $g(\Gamma_H)$ the genus of $X_H$ we have*

$$g(\Gamma_H) > 0.01 \frac{n^{2-\frac{0.96}{\log\log n}}}{\log\log n}.$$

*Proof.* Since $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then $X_H = \Gamma_H \backslash \overline{\mathbb{H}}$. Given a congruence subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$ containing $-\mathrm{Id}$, we denote by $d(\Gamma)$ the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Moreover, we denote by $\varepsilon_\infty(\Gamma)$ the number of cusps of $\Gamma\backslash\overline{\mathbb{H}}$ and by $\varepsilon_2(\Gamma)$, respectively $\varepsilon_3(\Gamma)$, the number of elliptic points of period 2, respectively 3, of $\Gamma\backslash\overline{\mathbb{H}}$. Then, by [DS05, Theorem 3.1.1], the genus of $\Gamma\backslash\overline{\mathbb{H}}$ is

$$g(\Gamma) = 1 + \frac{d(\Gamma)}{12} - \frac{\varepsilon_2(\Gamma)}{4} - \frac{\varepsilon_3(\Gamma)}{3} - \frac{\varepsilon_\infty(\Gamma)}{2}. \tag{3.13}$$

The numbers $d(\Gamma), \varepsilon_\infty(\Gamma), \varepsilon_2(\Gamma)$ and $\varepsilon_3(\Gamma)$ are multiplicative with the following meaning: Given two coprime integers $n_1, n_2$ and two congruence subgroups $\Gamma_1, \Gamma_2 < \mathrm{SL}_2(\mathbb{Z})$ of level $n_1$ and $n_2$ respectively, both containing $-\mathrm{Id}$, then

$$\begin{aligned} d(\Gamma_1 \cap \Gamma_2) &= d(\Gamma_1)d(\Gamma_2), & \varepsilon_\infty(\Gamma_1 \cap \Gamma_2) &= \varepsilon_\infty(\Gamma_1)\varepsilon_\infty(\Gamma_2), \\ \varepsilon_2(\Gamma_1 \cap \Gamma_2) &= \varepsilon_2(\Gamma_1)\varepsilon_2(\Gamma_2), & \varepsilon_3(\Gamma_1 \cap \Gamma_2) &= \varepsilon_3(\Gamma_1)\varepsilon_3(\Gamma_2). \end{aligned} \tag{3.14}$$

Let $n = p_1^{e_1} \cdots p_k^{e_k}$ the prime factorization of $n$ and we denote by $H_j$ the reduction of $H$ modulo $p_j^{e_j}$. Then each $H_j$ is either a Cartan or a Cartan-plus subgroup and, under the isomorphism $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{j=1}^k \mathrm{GL}_2(\mathbb{Z}/p_j^{e_j}\mathbb{Z})$, we have $H \cong \prod_{j=1}^k H_j$ and therefore $\Gamma_H = \bigcap_{j=1}^k \Gamma_{H_j}$. Last equation, together with the multiplicativity and (3.13), implies that we can estimate the genus of $X_H$ estimating the quantities $d(\Gamma_H), \varepsilon_\infty(\Gamma_H), \varepsilon_2(\Gamma_H)$ and $\varepsilon_3(\Gamma_H)$ for $n = p^e$. We write these values in Table 3.1. The numbers $\varepsilon_\infty(\Gamma_H), \varepsilon_2(\Gamma_H)$ and $\varepsilon_3(\Gamma_H)$ can be computed determining, for each representative $r$ of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_H$, the ramification index $[\mathrm{SL}_2(\mathbb{Z})_\tau : r^{-1}\Gamma_H r \cap (\Gamma_H)_\tau]$ at $\mathrm{SL}_2(\mathbb{Z})\tau$, for $\tau \in \overline{\mathbb{H}}$, of the $j$-map $j\colon X_H \to \mathrm{SL}_2(\mathbb{Z})\backslash\overline{\mathbb{H}}$, where $(\Gamma_H)_\tau$ is the stabilizer of $\tau$ in $\Gamma_H$. The only non-trivial $\tau$ to check, i.e., those such that $\mathrm{SL}_2(\mathbb{Z})_\tau$ is non-trivial, are $\tau \in \{i, e^{\frac{2\pi i}{3}}, \infty\} \cup \mathbb{Q}$. See [DS05, Sections 3.7 and 3.8] and [DMS19, Section 4.1] for the split case and [Bar10, Proposition 7.10] for the non-split case. In the proof of [Bar10, Proposition 7.10] there is also an explanation of the general method to carry on these calculations. The table implies that for every prime $p_j$ dividing $n$ with exponent $e_j$ we have

$$d(\Gamma_{H_j}) \geqslant \tfrac{1}{2}p_j^{2e_j}(1 - \tfrac{1}{p_j}), \quad \varepsilon_2(\Gamma_{H_j}) \leqslant p_j^{e_j}, \quad \varepsilon_3(\Gamma_{H_j}) \leqslant 2, \quad \varepsilon_\infty(\Gamma_{H_j}) \leqslant p_j^{e_j}(1 + \tfrac{1}{p_j}).$$

Table 3.1. Degree, elliptic points and cusps for prime power levels.

| $H$ | $d(\Gamma_H)$ | $\varepsilon_2(\Gamma_H)$ | $\varepsilon_3(\Gamma_H)$ | $\varepsilon_\infty(\Gamma_H)$ |
|---|---|---|---|---|
| $C_{\mathrm{s}}(p^e)$ | $p^{2e-1}(p+1)$ | 2 if $p \equiv 1 \bmod 4$<br>0 if $p \not\equiv 1 \bmod 4$ | 2 if $p \equiv 1 \bmod 3$<br>0 if $p \not\equiv 1 \bmod 3$ | $p^{e-1}(p+1)$ |
| $C_{\mathrm{s}}^+(p^e)$ | $\frac{p^{2e-1}(p+1)}{2}$ | $2^{e-1}$ if $p = 2$<br>$1+\frac{p^{e-1}(p-1)}{2}$ if $p \equiv 1 \bmod 4$<br>$\frac{p^{e-1}(p+1)}{2}$ if $p \equiv 3 \bmod 4$ | 1 if $p \equiv 1 \bmod 3$<br>0 if $p \not\equiv 1 \bmod 3$ | 2 if $p^e = 2$<br>$\frac{p^{e-1}(p+1)}{2}$ |
| $C_{\mathrm{ns}}(p^e)$ | $p^{2e-1}(p-1)$ | 0 if $p \not\equiv 3 \bmod 4$<br>2 if $p \equiv 3 \bmod 4$ | 0 if $p \not\equiv 2 \bmod 3$<br>2 if $p \equiv 2 \bmod 3$ | $p^{e-1}(p-1)$ |
| $C_{\mathrm{ns}}^+(p^e)$ | $\frac{p^{2e-1}(p-1)}{2}$ | $2^{e-1}$ if $p = 2$<br>$\frac{p^{e-1}(p-1)}{2}$ if $p \equiv 1 \bmod 4$<br>$1+\frac{p^{e-1}(p+1)}{2}$ if $p \equiv 3 \bmod 4$ | 0 if $p \not\equiv 2 \bmod 3$<br>1 if $p \equiv 2 \bmod 3$ | 1 if $p^e = 2$<br>$\frac{p^{e-1}(p-1)}{2}$ |

These inequalities and the multiplicativity (3.14) imply the following estimates for $n \geqslant 15$:

$$d(\Gamma_H) \geqslant \frac{n\phi(n)}{2^{\omega(n)}} > \frac{n^2}{4.4\,\log\log(n)2^{\omega(n)}} \geqslant \frac{n^2}{4.4\,\log\log(n)2^{1.3841\frac{\log n}{\log\log n}}} > \frac{n^{2-\frac{0.96}{\log\log n}}}{4.4\,\log\log n},$$

$$\varepsilon_2(\Gamma_H) \leqslant n, \quad \varepsilon_3(\Gamma_H) \leqslant 2^{\omega(n)} \leqslant n, \quad \varepsilon_\infty(\Gamma_H) \leqslant n\prod_{j=1}^{k}(1+\tfrac{1}{p_j}) \leqslant \sigma_1(n) \leqslant 2.59n\log\log n,$$

where $\phi(n)$ is Euler's totient function which is estimated using [RS62, Theorem 15], $\omega(n) = k$ is the number of prime divisors of $n$ which is estimated as in [Rob83a, Théorème 11], and $\sigma_1(n)$ is the sum of positive divisors of $n$ which is estimated as in [Ivi77, Theorem 1]. For $n \geqslant 10^5$, substituting in (3.13), we get

$$g(\Gamma_H) > 1 + \frac{n^{2-\frac{0.96}{\log\log n}}}{52.8\,\log\log n} - \frac{n}{3} - \frac{n}{4} - 1.3n\log\log n \geqslant 0.01\frac{n^{2-\frac{0.96}{\log\log n}}}{\log\log n}.$$

□

## 4. Field of definition of automorphisms

In this section we prove that, when the level is large enough, every automorphism of the modular curve $X_H$ associated to a subgroup $H$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is defined over the compositum of some quadratic fields, and in some cases we find explicitly this field.

Whenever $K$ is a field, $X$ is a variety over $K$, and $F$ is an extension of $K$, we write $\mathrm{Aut}_F(X)$ for the set of automorphisms of $X$ defined over $F$; analogously we use the notations $\mathrm{End}_F(X)$ and $\mathrm{Hom}_F(X, Y)$ for $X$ and $Y$ being abelian varieties over $K$. Whenever we omit the dependency on the field, we mean automorphisms (or endomorphisms) defined over the algebraic closure of $K$; in particular when $X$ is a modular curve the "group of the automorphisms of X" is $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X)$ or equivalently $\mathrm{Aut}_{\mathbb{C}}(X)$. We start with a straightforward generalization of [KM88, Lemma 1.4].

**Lemma 4.1.** *Let $K$ be a perfect field with algebraic closure $\overline{K}$, let $X$ be a smooth projective and geometrically connected curve defined over $K$ of genus $g(X)$ and let $\mathrm{Jac}(X)$ be its jacobian variety. We suppose that there are two abelian varieties $A_1$ and $A_2$ over $K$ such that $\mathrm{Hom}_{\overline{K}}(A_1, A_2) = 0$ and such that $\mathrm{Jac}(X)$ is isogenous over $K$ to $A_1 \times_K A_2$. If*

$$g(X) > 2\dim(A_2) + 1,$$

*and if $F \subset \overline{K}$ is an extension of $K$ such that $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$, then every automorphism of $X$ over $\overline{K}$ can be defined over $F$.*

*Proof.* We fix isogenies $\varphi\colon \mathrm{Jac}(X) \to A_1 \times_K A_2$ and $\varphi^\vee\colon A_1 \times_K A_2 \to \mathrm{Jac}(X)$ whose compositions are multiplications by an integer. Let $u \in \mathrm{Aut}_{\overline{K}}(X)$ and $\sigma \in \mathrm{Gal}(\overline{K}/F)$ and consider the automorphism $v := u^\sigma \circ u^{-1}$. Let $Y$ be the quotient of $X$ by the subgroup of automorphisms generated by $v$ (which is finite since $g(X) \geqslant 2$) and let $\mathrm{Jac}(Y)$ be the jacobian of $Y$. Because of $\varphi$, and since $\mathrm{Hom}_{\overline{K}}(A_1, A_2) = 0$, we can identify $u_*, u_*^\sigma \in \mathrm{Aut}_{\overline{K}}(\mathrm{Jac}(X))$ respectively with

$$(u_1, u_2), (u_1^\sigma, u_2^\sigma) \in (\mathrm{End}_{\overline{K}}(A_1) \otimes \mathbb{Q})^\times \times (\mathrm{End}_{\overline{K}}(A_2) \otimes \mathbb{Q})^\times \cong (\mathrm{End}_{\overline{K}}(A_1 \times_K A_2) \otimes \mathbb{Q})^\times.$$

Since $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$, then $u_1 = u_1^\sigma$, and $v_* = (\mathrm{id}, v_2)$.

This implies that

$$\dim(A_1) \leqslant \dim((A_1 \times_K A_2)^{(\mathrm{id}, v_2)}) \leqslant \dim(\mathrm{Jac}(X)^v),$$

where $\mathrm{Jac}(X)^v$ is the $v$-invariant subvariety of $\mathrm{Jac}(X)$. A point of $\mathrm{Jac}(X_{\overline{K}})^v$ is associated to a divisor $D$ on $X_{\overline{K}}$ which is equivalent to $vD$ in $\mathrm{Jac}(X_{\overline{K}})$. This implies, using the cyclicity of $\langle v\rangle$ and [GGJ05, Corollary 7], that every element of $\mathrm{Jac}(X_{\overline{K}})^v$ is represented by a $v$-invariant divisor on $X_{\overline{K}}$. This means that $\mathrm{Jac}(X_{\overline{K}})^v$ is the image of the pullback map $\pi^*\colon \mathrm{Jac}(Y_{\overline{K}}) \to \mathrm{Jac}(X_{\overline{K}})$. So we have that

$$\dim(\mathrm{Jac}(X)^v) = \dim(\mathrm{Jac}(X_{\overline{K}})^v) = \dim(\mathrm{Jac}(Y_{\overline{K}})) = g(Y),$$

where $g(Y)$ is the genus of $Y$, and, therefore, we have

$$g(X) - \dim(A_2) = \dim(A_1) \leqslant g(Y).$$

Hence, by the Riemann-Hurwitz formula applied to the projection $X \to Y$, we have

$$\dim(A_1) + \dim(A_2) - 1 \geqslant d(g(Y) - 1) \geqslant d\dim(A_1) - d,$$

where $d$ is the order of $v$. If $d > 1$, we get $\dim(A_1) \leqslant \dim(A_2) + 1$, which is impossible by hypothesis. Hence $d = 1$ and $v$ is the identity. This implies that $u^\sigma = u$, for every $\sigma \in \mathrm{Gal}(\overline{K}/F)$, i.e., since $K$ is perfect, $u \in \mathrm{Aut}_F(X)$. □

For every abelian variety $A$ over a number field $K$, let $A^{\mathrm{C}}$ be the maximal abelian subvariety of $A_{\overline{K}}$ that is isogenous to a product of simple CM abelian varieties and let $A^{\mathrm{N}}$ be the maximal abelian subvariety of $A_{\overline{K}}$ that is isogenous to a product of simple non-CM abelian varieties. We call $A^{\mathrm{C}}$ the CM-part of $A$ and $A^{\mathrm{N}}$ the non-CM-part of $A$. Both the CM part and the non-CM part of $A$ are also defined $K$, since by definition we have $(A^{\mathrm{C}})^\tau = A^{\mathrm{C}}$ and $(A^{\mathrm{N}})^\tau = A^{\mathrm{N}}$ for each $\tau \in \mathrm{Gal}(\overline{K}/K)$. The dimension of the CM-part and the dimension of the non-CM part are invariant under isogeny on $A$. Hence, by looking at the decomposition of $A$ in simple factors, we see that $\dim(A^{\mathrm{C}}) + \dim(A^{\mathrm{N}}) = \dim(A)$.

We want to apply Lemma 4.1 to the case $A_1 = \mathrm{Jac}(X)^{\mathrm{N}}$ and $A_2 = \mathrm{Jac}(X)^{\mathrm{C}}$. Hence, we are interested in an upper bound on the dimension of the CM part of the jacobian of Cartan modular curves. By Theorem 3.8, it is enough to know an upper bound in the case $X = X_0(n)$.

**Proposition 4.2.** *For every integer $n > 1$, the dimension $g_0^{\mathrm{C}}(n)$ of the CM part of $J_0(n)$ satisfies*

$$g_0^{\mathrm{C}}(n) \leqslant 9\log(n)^2 n^{\frac{1}{2}+\frac{2.816}{\log\log n}}.$$

*Proof.* For every positive integer $k$, let $J_0^{\mathrm{new}}(k)$ be the new part of $J_0(k)$ and let $\sigma_0(k)$ be the number of positive divisors of $k$. Then we have a canonical isogeny

$$J_0(n) \sim \prod_{d|n} J_0^{\mathrm{new}}(d)^{\sigma_0(n/d)}.$$

Denoting by $g_0^{\mathrm{new,C}}(d)$ the dimension of the CM part of $J_0^{\mathrm{new}}(d)$, we also have

$$g_0^{\mathrm{C}}(n) = \sum_{d|n} \sigma_0(n/d) g_0^{\mathrm{new,C}}(d). \tag{4.3}$$

We know that $J_0^{\mathrm{new}}(d)$ is isogenous over $\mathbb{Q}$ to $\prod_{[f]} A_f$, where $[f]$ is the Galois orbit of the newform $f$, and the cardinality of $[f]$ is equal to the dimension of $A_f$ (see [DS05, Chapter 6]). We now look at the CM part of each factor $A_f$.

In order to do this, we describe a bijection between the set of normalized newforms contributing to the CM part and a suitable set of triples $(K, \mathfrak{m}, \lambda)$, where $K$ is an imaginary quadratic field, $\mathfrak{m}$ is an ideal of the ring of integers $\mathcal{O}_K$ of $K$ and $\lambda$ is a primitive Grössencharacter of $K$ defined modulo $\mathfrak{m}$ (see [Shi71b, Section 4] for the definition of primitive

Grössencharacter). Namely, let $(K, \mathfrak{m}, \lambda)$ be a triple as above such that the nebentypus associated to $\lambda$ is trivial and let $\Delta_K$ be the discriminant of $K$, then, by [Shi71b, Lemma 3 and Theorem 1], we can construct a normalized newform $f_\lambda$ of level $|\Delta_K||\mathfrak{m}|$ such that the associated abelian variety $A_{f_\lambda}$ is isogenous over $\mathbb{C}$ to a product of elliptic curves with CM over $K$. On the other hand, by [Shi72, Proposition 1.6], for each normalized newform $f$, if the associated abelian variety $A_f$ has non-trivial CM part, then $f = f_\lambda$ for a unique triple $(K, \mathfrak{m}, \lambda)$ as above. This gives a bijection between the set of normalized newforms $f$ contributing to the CM part of $J_0^{\text{new}}(d)$ and the set of triples $(K, \mathfrak{m}, \lambda)$ described above such that $|\Delta_K||\mathfrak{m}| = d$. By [Shi72, Proposition 1.6], an abelian variety $A_f$ has non-trivial CM part if and only if it is isogenous over $\mathbb{C}$ to a product of elliptic curves with CM over $K$. Hence the number of normalized newforms $f$ of level $d$ contributing to the CM part is equal to the dimension of the CM part of $J_0^{\text{new}}(d)$. In conclusion, $g_0^{\text{new,C}}(d)$ is equal to the number of triples $(K, \mathfrak{m}, \lambda)$ where $\lambda$ is a primitive Grössencharacter of $K$ defined modulo $\mathfrak{m}$ with trivial nebentypus and $|\Delta_K||\mathfrak{m}| = d$.

We now give an upper bound on the number of such triples. For every choice of $K$ and $\mathfrak{m}$, the set of primitive Grössencharacters of $K$ defined modulo $\mathfrak{m}$ is a subset of the set of Grössencharacters of $K$ defined modulo $\mathfrak{m}$. If this set is not empty, then there is at least one Grössencharacter $\lambda_0$ and all other Grössencharacters are given by $\lambda_0\chi$, for $\chi$ a character of the group

$$\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) := \frac{\{\text{fractional ideals of } \mathcal{O}_K \text{ coprime to } \mathfrak{m}\}}{\{(\alpha) : \exists a \in \mathbb{Z} \text{ coprime to } \mathfrak{m} \text{ such that } \alpha \equiv a \bmod \mathfrak{m}\}}.$$

Thus, for given $K$ and $\mathfrak{m}$, the cardinality of $\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)$ is larger than the number of triples $(K, \mathfrak{m}, \lambda)$ we are interested in, hence

$$g_0^{\text{new,C}}(d) \leqslant \sum_{|\Delta_K||\mathfrak{m}|=d} \#\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)\,. \tag{4.4}$$

To give a bound on $\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)$ we look at the following short exact sequence

$$1 \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m})^\times}{\mathcal{O}_K^\times \cdot (\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times} \longrightarrow \widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 0,$$

where $\mathrm{Cl}(K)$ is the class group of $K$ and we write $\mathcal{O}_K^\times$ and $(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times$ in place of their natural image inside $(\mathcal{O}_K/\mathfrak{m})^\times$. We write $\mathfrak{m} = \prod_p \mathfrak{m}_p$ for $p$ varying in the set of rational primes and $\mathfrak{m}_p$ being a product of primes of $\mathcal{O}_K$ dividing $p$. Thus the above short exact sequence gives

$$\#\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) \leqslant \#\mathrm{Cl}(K)\cdot\#\left(\frac{(\mathcal{O}_K/\mathfrak{m})^\times}{(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times}\right) = \#\mathrm{Cl}(K)\prod_{p\mid|\mathfrak{m}|}\#\left(\frac{(\mathcal{O}_K/\mathfrak{m}_p)^\times}{(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}_p))^\times}\right) \leqslant$$
$$\leqslant 3\log(|\Delta_K|)\sqrt{|\Delta_K|}\prod_{p\mid|\mathfrak{m}|}\left((1+\tfrac{1}{p})|\mathfrak{m}_p|^{1/2}\right) = 3\log(|\Delta_K|)\sqrt{|\Delta_K||\mathfrak{m}|}\prod_{p\mid|\mathfrak{m}|}(1+\tfrac{1}{p}),$$

where the class number of $K$ is estimated using [Nar04, Theorem 8.10 and Lemma 8.16] and the bound on the cardinality of $(\mathcal{O}_K/\mathfrak{m}_p)^\times/(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}_p))^\times$ is trivial after factoring $\mathfrak{m}_p$. Substituting in (4.4), we have

$$g_0^{\text{new,C}}(d) \leqslant \sum_{|\Delta_K||\mathfrak{m}|=d}\left(3\sqrt{d}\log(|\Delta_K|)\prod_{p\mid|\mathfrak{m}|}(1+\tfrac{1}{p})\right).$$

Let $M_d := \#\Big\{(K,\mathfrak{m}) : |\Delta_K||\mathfrak{m}| = d\Big\}$ and for $m \in \mathbb{Z}_{\geqslant 1}$, we denote by $\sigma_1(m)$ the sum of the positive divisors of $m$. We have $\sigma_1(m) < 3m\log m$, for each $m \geqslant 2$ (see [Ivi77, Theorem 1] if $m \geqslant 7$, it is trivial in the remaining cases). Then

$$g_0^{\text{new,C}}(d) \leqslant 3M_d\sqrt{d}\log(d)\prod_{p|d}(1+\tfrac{1}{p}) \leqslant 3M_d\sqrt{d}\log(d)\tfrac{\sigma_1(d)}{d} \leqslant 9M_d\sqrt{d}\log(d)^2.$$

Substituting in (4.3), we get

$$\begin{aligned} g_0^{\text{C}}(n) &\leqslant 9\sum_{d|n}\sigma_0(n/d)M_d\sqrt{d}\log(d)^2 \leqslant 9\sqrt{n}\log(n)^2\sum_{d|n}M_d\sigma_0(n/d) \leqslant \\ &\leqslant 9\sqrt{n}\log(n)^2\#\Big\{(K,\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}. \end{aligned} \tag{4.5}$$

Writing the prime factorization $n = \prod_{i=1}^r p_i^{e_i}$, we know that an imaginary quadratic field $K$ with discriminant dividing $n$ must be $K = \mathbb{Q}(\sqrt{-\prod_{i=1}^r p_i^{\varepsilon_i}})$, with $\varepsilon \in \{0,1\}^r$. Hence

$$\#\Big\{(K,\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\} \leqslant \sum_{\varepsilon\in\{0,1\}^r}\#\Big\{(\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\} \leqslant$$

$$\leqslant \sum_{\substack{\varepsilon\in\{0,1\}^r \\ m\in\mathbb{Z}_{>0}}}\#\Big\{\mathfrak{m}\subset\mathcal{O}_K : |\mathfrak{m}| = m\Big\}\cdot\#\Big\{d\in\mathbb{Z}_{>0} : dm\prod_{i=1}^r p_i^{\varepsilon_i} \text{ divides } n\Big\}.$$

We have the factorizations $m = \prod_{i=1}^r p_i^{f_i}$ and $d = \prod_{i=1}^r p_i^{c_i}$, where $f_i, c_i \in \{0,1,\ldots,e_i\}$, for $i = 1,\ldots,r$, and we denote by $f$ the $r$-tuple whose components are the $f_i$'s and similarly we define $c$. Then the number of ideals $\mathfrak{m}$ in $\mathcal{O}_K$ having norm $m$ is lesser than $\prod_{i=1}^r(f_i+1)$ which is equal to the number of pairs $(a,b)$ of elements of $\mathbb{Z}_{\geqslant 0}^r$ such that $a+b = f$. Hence we get

$$\#\Big\{(K,\mathfrak{m},d){:}|\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}{\leqslant}\#\Big\{(\varepsilon,a,b,c)\in\{0,1\}^r{\times}(\mathbb{Z}_{\geqslant 0}^r)^3{:}\ \varepsilon_i + a_i{+}b_i{+}c_i \leqslant e_i\Big\}{\leqslant}$$

$$\leqslant\prod_{i=1}^r\Big(\#\Big\{(a_i,b_i,c_i)\in\mathbb{Z}_{\geqslant 0}^3 : a_i{+}b_i{+}c_i \leqslant e_i\Big\} + \#\Big\{(a_i,b_i,c_i)\in\mathbb{Z}_{\geqslant 0}^3 : a_i{+}b_i{+}c_i \leqslant e_i{-}1\Big\}\Big){\leqslant}$$

$$\leqslant\prod_{i=1}^r\left(\binom{e_i+3}{3} + \binom{e_i+2}{3}\right){\leqslant}\prod_{i=1}^r\frac{(e_i+2)(e_i+1)^2}{2}.$$

Notice that $\sigma_0(n) = \prod_{i=1}^r(e_i{+}1)$ is the number of positive divisors of $n$ and $\prod_{i=1}^r\frac{(e_i+2)(e_i+1)}{2}$ is the number of triples $(d_1,d_2,d_3)$ of positive integers such that $d_1d_2d_3 = n$. Using the upper bounds, contained in [NR83] and [Rob83b], for these two quantities, we get

$$\#\Big\{(K,\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\} \leqslant n^{\frac{1.538\log 2}{\log\log n}}n^{\frac{1.592\log 3}{\log\log n}} \leqslant n^{\frac{2.816}{\log\log n}}.$$

Substituting in (4.5) we find

$$g_0^{\text{C}}(n) \leqslant 9\sqrt{n}\log(n)^2n^{\frac{2.816}{\log\log n}} = 9\log(n)^2n^{\frac{1}{2}+\frac{2.816}{\log\log n}}.$$

□

When the level is a prime power, the previous upper bound is easier and smaller.

**Proposition 4.6.** *For every prime $p$ and positive integer $e$, the dimension $g_0^{\mathrm{C}}(p^e)$ of the CM part of $J_0(p^e)$ satisfies*

$$g_0^{\mathrm{C}}(p^e) \leqslant \begin{cases} 13\sqrt{2^e} & \text{if } p = 2, \\ 0 & \text{if } p \equiv 1 \bmod 4, \\ 5.5\sqrt{p^e}\log p & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

The proof follows the same steps of the previous proposition and is simplified by the fact that there are few quadratic imaginary fields $K$ whose discriminant divides $p^e$. More precisely: there are two fields when $p = 2$, there are no fields if $p \equiv 1 \bmod 4$ and there is only one field if $p \equiv 3 \bmod 4$. We now give an upper bound for the field of definition of the automorphisms of a Cartan modular curve of large enough level.

**Proposition 4.7.** *Let $n \geqslant 10^{400}$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of $X_H$ is defined over the compositum of all the quadratic fields whose discriminant divides $n$.*

*Proof.* Let $J_H$ be the jacobian of $X_H$ and let $J_H^{\mathrm{C}}$ and $J_H^{\mathrm{N}}$ be the CM part and the non-CM part of $J_H$ respectively. By Lemma 4.1, it is enough to prove that $2\dim(J_H^{\mathrm{C}})+1$ is smaller than the genus of $X_H$ and that every endomorphism of $J_H^{\mathrm{N}}$ is defined over the compositum of all the quadratic fields whose discriminant divides $n$. The latter is true because, by Theorem 3.8, $J_H^{\mathrm{N}}$ is a quotient of $J_0(n^2)^{\mathrm{N}}$ and by in [KM88, Proposition 1.3] every endomorphism of $J_0(n^2)^{\mathrm{N}}$ is defined over the compositum of all the quadratic fields whose discriminant divides $n$. By Theorem 3.8 $J_H^{\mathrm{C}}$ is a quotient of $J_0(n^2)^{\mathrm{C}}$ hence we can use Proposition 4.2 to bound the $\dim(J_H^{\mathrm{C}})$; this, together with the bound for the genus $g(X_H)$ of $X_H$ given in Proposition 3.12, implies the inequality we need when $n \geqslant 10^{400}$:

$$2\dim(J_H^{\mathrm{C}}) + 1 \leqslant 2\dim(J_0(n^2)^{\mathrm{C}}) + 1 \leqslant 73\log(n)^2 n^{1+\frac{5.632}{\log\log n}} < \frac{n^{2-\frac{0.96}{\log\log n}}}{100\log\log n} < g(X_H).$$

□

Proposition 4.7 can be made sharper when $n$ is a prime power.

**Proposition 4.8.** *Let $p$ be a prime and $e$ a positive integer and let $X$ be a curve associated to a Cartan or a Cartan-plus subgroup of level $p^e$. If the genus of $X$ is at least 2, then every automorphism of $X$ is defined over the field*

$$K_p = \begin{cases} \mathbb{Q}(i, \sqrt{2}), & \text{if } p = 2, \\ \mathbb{Q}\left(\sqrt{p}\right), & \text{if } p \equiv 1 \bmod 4, \\ \mathbb{Q}\left(\sqrt{-p}\right), & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

A strategy of proof is the same of Proposition 4.7:

(i) give an upper bound for $\dim(\mathrm{Jac}(X)^{\mathrm{C}})$;
(ii) give a lower bound for the genus;
(iii) apply [KM88, Proposition 1.3] and Theorem 3.8 to deduce that the endomorphisms of $\mathrm{Jac}(X)^{\mathrm{N}}$ are defined over $K_p$;
(iv) apply Lemma 4.1.

In particular in the case of $X_{\mathrm{ns}}(p^e)$ and $X_{\mathrm{ns}}^+(p^e)$, when $p^e > 600$, the propositions 3.6 and 4.6 and Table 3.1 give bounds in (i) and (ii) that are sharp enough for (iv). If $p^e \leqslant 600$, the bounds in Proposition 4.6 are sometimes not sharp enough. In these cases we can compute explicitly the CM part and notice that only a factor of it of low dimension has endomorphisms defined over a field bigger than $K_p$: whenever a CM factor is a rational elliptic curve, we know by CM theory that its endomorphisms are defined over $K_p$ and it can be discarded from the count. This is done in the MAGMA script available at [Scr]. The case $X_{\mathrm{s}}(p^e) \cong X_0(p^{2e})$ follows from [KM88, Corollary 1.14] and the case $X_{\mathrm{s}}^+(p^e) \cong X_0(p^{2e})$ follows from the following proposition.

**Proposition 4.9.** *Let $p$ be a prime and $e$ a positive integer. If the genus of $X_0^*(p^e)$ is at least 2, then every automorphism of $X_0^*(p^e)$ is defined over the field*

$$K_p = \begin{cases} \mathbb{Q}(i, \sqrt{2}), & \text{if } p = 2, \\ \mathbb{Q}\left(\sqrt{p}\right), & \text{if } p \equiv 1 \bmod 4, \\ \mathbb{Q}\left(\sqrt{-p}\right), & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Again, one can apply the same strategy used for Propositions 4.7 and 4.8, together with the MAGMA script available at [Scr]. In particular we need a lower bound for the genus of $X_0^*(p^e)$. Since we do not know an explicit reference giving a formula for this genus, we write it in the following remark.

*Remark* 4.10. Given a positive integer $n$, let $X_0^+(n)$ be the quotient of $X_0(n)$ by the $n$-th Atkin-Lehner operator. This curve is equal to $X_0^*(n)$ when $n$ is the power of a prime.

In [Ogg75b, Equation 9] there is a formula for the genus $g_0^+(n)$ of $X_0^+(n)$ when $n$ is prime. When $n = p^{2e}$ with $p$ prime, we can compute $g_0^+(n)$ using Table 3.1 since $X_0^+(n)$ is isomorphic to a split Cartan curve. For general $n$, [Ogg75b, Equation 9] can be easily generalized applying Riemann-Hurwitz formula to the natural map $X_0(n) \to X_0^+(n)$ and counting the number of fixed points of the $n$-th Atkin-Lehner operator. This gives

$$g_0^+(n) = \begin{cases} 0, & \text{if } n \in \{1, 2, 3, 4\}, \\ \frac{1+g_0(n)}{2} - \frac{h(-n)+h(-4n)}{4}, & \text{if } n \geqslant 5 \text{ is odd}, \\ \frac{1+g_0(n)}{2} - \frac{h(-4n)}{4}, & \text{if } n \geqslant 5 \text{ is even}, \end{cases}$$

where $g_0(n)$ is the genus of $X_0(n)$ and $h(D)$ is the class number of the quadratic order with discriminant $D$, with the convention $h(D) = 0$ if $D$ is a square or if $D \equiv 2, 3 \bmod 4$.

*Remark* 4.11. We are not always able to prove that every automorphism of a Cartan modular curve is defined over a compositum of quadratic fields. For example, an analogous of Equation (3.9) for Cartan-plus curves, proved using Chen's isogeny in [Che04], implies that the jacobian of the totally non-split Cartan-plus curve $X$ of level 48 contains $J_0^{\mathrm{new},*}(48^2)$. Since there are two CM (weight 2) newforms of level $48^2$ of degree 2 and invariant under the action of both the Atkin-Lehner operators $w_9$ and $w_{256}$, then the jacobian $J_0^{\mathrm{new},*}(48^2)$ has a CM part of dimension at least 4 whose endomorphisms could be defined over a field bigger than the compositum of quadratic fields. This prevents us from applying Lemma 4.1 in (iv) of the strategy above, because the genus of $X$ is 9 (see Table 3.1).

## 5. Automorphisms

In this section we treat our main problem, namely to determine the automorphisms of certain modular curves $X_H$ over $\mathbb{C}$ for a subgroup $H$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We restrict our attention to $X_H$ geometrically connected, i.e., $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. Every automorphism we are interested in induces an automorphism of the Riemann surface $X_H(\mathbb{C}) = \Gamma_H \backslash \overline{\mathbb{H}}$

and, since it is compact, each of these automorphisms comes from an automorphism of the algebraic curve $(X_H)_{\mathbb{C}}$. Let $\mathbb{P}\colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q})$ be the natural map. Each matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ defines a Möbius transformation $m\colon \overline{\mathbb{H}} \to \overline{\mathbb{H}}$ and such an automorphism of the Riemann surface $\overline{\mathbb{H}}$ pushes down to an automorphism of $\Gamma_H\backslash\overline{\mathbb{H}}$ if and only if $m$ normalizes $\mathbb{P}(\Gamma_H)$.

**Definition 5.1.** Let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. An automorphism of $X_H$ defined over $\mathbb{C}$ is *modular* if its action on $X_H(\mathbb{C}) = \Gamma_H\backslash\overline{\mathbb{H}}$ is described by a Möbius transformation associated to a matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ normalizing $\mathbb{P}(\Gamma_H)$.

When $H$ has surjective determinant, $\mathrm{Aut}(X_H)$ contains the subgroup of modular automorphisms which is isomorphic to $\mathcal{N}/\mathbb{P}(\Gamma_H)$, where $\mathcal{N}$ is the normalizer of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$.

*Remark* 5.2. Notice that we can define modular automorphisms of $Y_H$ looking at $\mathrm{PGL}_2^+(\mathbb{R})$, instead of $\mathrm{PGL}_2^+(\mathbb{Q})$, as follows: an automorphism $\iota$ of $Y_H(\mathbb{C}) = \Gamma_H\backslash\mathbb{H}$ is *modular* if there is a matrix $m \in \mathrm{PGL}_2^+(\mathbb{R})$ that normalizes the image of $\Gamma_H$ in $\mathrm{PGL}_2^+(\mathbb{R})$ and hence defines a Möbius transformation $m\colon \mathbb{H} \to \mathbb{H}$ that pushes down to $\iota$. This is equivalent to the previous definition. Indeed if $\tilde{m} \in \mathrm{GL}_2^+(\mathbb{R})$ is a lift of $m$, then $\tilde{m}$ normalizes $\Gamma_{\pm H} = (\mathbb{R}^\times\Gamma_H) \cap \mathrm{SL}_2(\mathbb{R})$, hence conjugation by $\tilde{m}$ preserves the set of $\mathbb{Q}$-linear combinations of matrices in $\Gamma_{\pm H}$, which is equal to the set of matrices with entries in $\mathbb{Q}$. Looking at the conjugates by $\tilde{m}$ of the matrices $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we easily deduce that $\tilde{m}$ is a real multiple of a matrix in $\mathrm{GL}_2(\mathbb{Q})$, and consequently $m$ lies in $\mathrm{PGL}_2^+(\mathbb{Q})$.

In other words: every modular automorphism of $Y_H(\mathbb{C})$ extends to a modular automorphism of $X_H$ and, conversely, every modular automorphism of $X_H$ preserves the set of cusps, hence restricts to a modular automorphism of $Y_H(\mathbb{C})$.

If an automorphism is modular, then it preserves the set of cusps and the set of branch points for the map $\mathbb{H} \to \Gamma_H\backslash\mathbb{H}$, because the map $\overline{\mathbb{H}} \to X_H(\mathbb{C})$ is branched on these sets and $\mathbb{P}^1(\mathbb{Q})$ is stable under $\mathrm{PGL}_2(\mathbb{Q})$. The converse is also true, as shown in [Dos16, Proposition 3.1]. In the following lemma we use this criterion to give a (different) sufficient condition for an automorphism to be modular.

**Lemma 5.3.** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the scalar matrices and such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, and let $\mathrm{gon}(X_H)$ be the gonality of $X_H$. If there is a prime $\ell$ not dividing $n$ such that $5 \leqslant \ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then every automorphism of $X_H$ defined over a compositum of quadratic fields is modular.*

*Proof.* Let $u$ be an automorphism of $X_H$ defined over the compositum of some quadratic fields and let $P \in X_H(\mathbb{C})$ be either a cusp or a branch point of the map $\mathbb{H} \to \Gamma_H\backslash\mathbb{H} = Y_H(\mathbb{C})$. By Proposition 1.6, if $P$ is branch point, then we have either $P = (E_i, \phi)$ with $\phi^{-1}\circ i|_{E_i[n]}\circ\phi \in \pm H$ or $P = (E_\rho, \phi)$ with $\phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi \in \pm H$. Hence, in both cases (cusp or branch point) we can apply Theorem 2.4 and deduce which particular multiplicities appear in $T_\ell(P)$: depending on the case, $T_\ell(P)$ contains either a point with multiplicity at least 4 or a point with multiplicity 3 or two distinct points with multiplicity 2. Since $u$ is defined over a compositum of quadratic fields and $\ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$, we can apply Proposition 2.2 to deduce that $T_\ell(P)$ and $T_\ell u(P)$ have the same “shape”. Since $u$ is defined over a compositum of quadratic fields and $\ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$, we can apply Proposition 2.2 to deduce that, under the definition of $\sigma$ given in the same proposition,

$T_\ell u(P) = u^\sigma T_\ell(P)$, hence the same coefficients appear in the divisors $T_\ell u(P)$ and $T_\ell(P)$, since $u^\sigma$ is an automorphism. Hence, applying Theorem 2.4 once again, we have that $u(P)$ is a cusp if $P$ is a cusp and $u(P)$ is a branch point if $P$ is branch point.

Therefore we proved that $u$ preserves the set of cusps and the set of branch points. Applying [Dos16, Proposition 3.1], we obtain that $u$ is induced by an automorphism $v\colon \mathbb{H} \to \mathbb{H}$. We know that $\mathrm{Aut}(\mathbb{H}) = \mathrm{PGL}_2^+(\mathbb{R})$, hence $v$ is a Möbius transformation given by a matrix $m \in \mathrm{PGL}_2^+(\mathbb{R})$. Since it factors through the quotient, $m$ belongs to the normalizer of the image of $\Gamma_H$ in $\mathrm{PGL}_2^+(\mathbb{R})$. Hence the restriction of $u$ to $Y_H$ is modular and, by Remark 5.2, $u$ itself is modular. □

We still need to determine which are the modular automorphisms of a modular curve $X_H$ for Cartan and Cartan-plus subgroups $H$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Since in these cases we have $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then $Y_H$ also parametrizes pairs $(E, \phi)$ such that the Weil pairing of $(\phi\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \phi\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right))$ is fixed, up to the action of $H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. With this interpretation, every matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ that normalizes $H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ defines an automorphism of $Y_H$ sending $(E, \phi) \mapsto (E, \phi \circ \gamma)$: such an automorphism is modular, induced by a lift of $\gamma$ in $\mathrm{SL}_2(\mathbb{Z})$. The next proposition implies that these are all the modular automorphisms except when $n \equiv 2 \bmod 4$ and $H$ is a Cartan-plus which is split at 2. We now suppose we are in this last case and we construct another modular automorphism. Letting $n = 2n'$, we have

$$H = H_2 \times H_{n'} \subset \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n'\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

where $H_2$ and $H_{n'}$ are the images of $H$ in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/n'\mathbb{Z})$ respectively. Since we are assuming that $H_2$ is a split Cartan-plus subgroup, there are three possibilities for $H_2$ (all conjugated) and, depending on them, we define

$$\gamma_0 := \begin{cases} \left(\begin{smallmatrix}3&1\\1&1\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\}, \\ \left(\begin{smallmatrix}2&2\\1&2\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\}, \\ \left(\begin{smallmatrix}2&1\\2&2\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\}. \end{cases} \tag{5.4}$$

Since the projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2n\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n'\mathbb{Z})$ is surjective and since $\det(H_{n'}) = (\mathbb{Z}/n'\mathbb{Z})^\times$, there exists

$$\gamma_1 \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{such that} \quad \gamma_1 \equiv \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \pmod 4 \quad \text{and} \quad (\gamma_1\gamma_0)^T \pmod{n'} \in H_{n'}. \tag{5.5}$$

The matrix $\mathbb{P}(\gamma_1\gamma_0)$ lies in the normalizer $\mathcal{N}$ of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$ and we have that $\mathbb{P}(\gamma_1\gamma_0)^2 \in \mathbb{P}(\Gamma_H)$, hence $\mathbb{P}(\gamma_1\gamma_0)$ induces an involution on $X_H$. Since $\mathbb{P}(\gamma_1\gamma_0) \notin \mathbb{P}(\mathrm{SL}_2(\mathbb{Z}))$, the modular automorphism defined by $\gamma_1\gamma_0$ is not of the form $(E, \phi) \mapsto (E, \phi \circ \gamma)$ with $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

**Proposition 5.6.** *Let $n$ be a positive integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan subgroup or a Cartan-plus subgroup. Let $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ be the normalizer of the group $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and let $\mathcal{N}$ be the normalizer of $\mathbb{P}(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$. If $n \equiv 2 \bmod 4$ and $H$ is a Cartan-plus split at 2, then, for every choice of $\gamma_0$ and $\gamma_1$ as in (5.4) and (5.5), $\mathcal{N}$ is generated by $\mathbb{P}(\Gamma_{N'})$ and $\mathbb{P}(\gamma_1\gamma_0)$. Otherwise $\mathcal{N}$ is $\mathbb{P}(\Gamma_{N'})$.*

*Proof.* Let $\tilde{\mathcal{N}} < \mathrm{GL}_2^+(\mathbb{Q})$ be the normalizer of $\mathbb{Q}^\times\Gamma_H$, or, equivalently, the normalizer of $\Gamma_H$ (each matrix normalizing $\mathbb{Q}^\times\Gamma_H$ also normalizes $(\mathbb{Q}^\times\Gamma_H) \cap \mathrm{SL}_2(\mathbb{Q}) = \Gamma_H$, and since scalar matrices commute with everything, each matrix normalizing $\Gamma_H$ also normalizes $\mathbb{Q}^\times\Gamma_H$). The conclusion of the proposition is equivalent to

$$\tilde{\mathcal{N}} = \mathbb{Q}^\times\Gamma_{N'} \quad \text{or} \quad \tilde{\mathcal{N}} = \mathbb{Q}^\times\langle\gamma_1\gamma_0, \Gamma_{N'}\rangle,$$

depending on the case. The inclusions $\supseteq$ are trivial, hence we prove the other inclusions. Since the normalizer of $\Gamma_H$ inside $\mathrm{SL}_2(\mathbb{Z})$ is $\Gamma_{N'}$, it is enough to show that

$$\tilde{\mathcal{N}} \subseteq \mathbb{Q}^\times \mathrm{SL}_2(\mathbb{Z}) \quad \text{or} \quad \tilde{\mathcal{N}} \subseteq \mathbb{Q}^\times \mathrm{SL}_2(\mathbb{Z}) \cup \gamma_1\gamma_0\mathbb{Q}^\times \mathrm{SL}_2(\mathbb{Z}),$$

depending on the case. We suppose that $\tilde{\mathcal{N}}$ contains a matrix $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ not lying in $\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$: it is enough to prove, with this assumption, that $n \equiv 2 \bmod 4$ and $H$ is a Cartan-plus subgroup split at 2 and $m \in \gamma_1\gamma_0\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$.

Up to multiplication by a scalar matrix, we can suppose that $a, b, c, d \in \mathbb{Z}$ and that $\gcd(a, b, c, d) = 1$. Since $m \notin \mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$, then $\det(m) \neq 1$. Let $p$ be a prime dividing $\det(m)$, let $\lambda_1 = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right), \lambda_2 = \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) \in \mathbb{Z}^2$ and let $\Lambda \subset \mathbb{Z}^2$ be the lattice generated by $\lambda_1, \lambda_2$. By definition of $\tilde{\mathcal{N}}$, for every $\gamma \in \Gamma_H$ there is $\gamma' = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \Gamma_H$ such that $\gamma m = m\gamma'$. Hence, looking at the columns of $\gamma m$, we get $\gamma\lambda_1 = x\lambda_1 + z\lambda_2$ and $\gamma\lambda_2 = y\lambda_1 + w\lambda_2$. Since $\gamma$ is arbitrary and $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$\Gamma_H\Lambda = \Lambda.$$

Let $\overline{\Lambda}$ be the image of $\Lambda$ under the quotient map $\mathbb{Z}^2 \to \mathbb{F}_p^2$. Since at least one of $a, b, c, d$ is not multiple of $p$, we know that $\overline{\Lambda} \neq \{0\}$ and since $\det(m)$ is multiple of $p$, we know that $\overline{\Lambda} \neq \mathbb{F}_p^2$. Hence $\overline{\Lambda}$ is a line inside $\mathbb{F}_p^2$ which is left invariant by every matrix in the image $\overline{\Gamma}_H$ of $\Gamma_H$ in $\mathrm{GL}_2(\mathbb{F}_p)$. This implies that $\overline{\Gamma}_H$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, thus $p$ divides the level $n$ and $\overline{\Gamma}_H = \overline{H}^T \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, where $\overline{H}$ is the image of $H$ in $\mathrm{GL}_2(\mathbb{F}_p)$. We deduce that either $H$ is a Cartan group split at $p$ or $p = 2$ and $H$ is a Cartan-plus group split at $p$.

First we suppose that $H$ is a Cartan group split at $p$. Let $p^e$ be the maximum power of $p$ dividing $n$. Up to conjugacy, the image of $H$ in $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\}$, hence $m^{-1}\gamma m \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \pmod{p^e}$, as $\gamma \in \Gamma_H$. Applying this to $\gamma = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ and $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$, we see, since $\det(m)$ is a multiple of $p$, that $p \mid a, b, c, d$, which is a contradiction.

This contradiction implies that the only prime dividing $\det(m)$ is 2 and $H$ is a Cartan-plus group split at 2. Let $2^e$ be the maximum power of 2 dividing $n$. Up to conjugacy, the image of $H$ in $\mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$ is $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}$. In particular the image of $H$ in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is $\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$, hence $\overline{\Lambda} = \langle\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)\rangle$ is the only $\overline{\Gamma}_H$-invariant line. With a similar argument we see that the rows $(a\,b), (c\,d)$ of $m$ span $\langle(1\,1)\rangle$ in $\mathbb{F}_2^2$. Hence $m \equiv \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \pmod 2$. For every $\gamma \in \Gamma_H$, we have

$$m^{-1}\gamma m \pmod{2^e} \in \{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}. \tag{5.7}$$

When $\gamma = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, we see that $m^{-1}\gamma m \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \pmod{2^e}$ is not possible because both $c$ and $d$ are odd, hence $m^{-1}\gamma m \equiv \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right) \pmod{2^e}$ and, by explicit computations, we deduce that $\det(m) = 2$ and $n \equiv 2 \bmod 4$. Finally, since $m \equiv \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \pmod 2$ and $\det(m) = 2$, we see that $(\gamma_1\gamma_0)^{-1}m \in \mathrm{SL}_2(\mathbb{Z})$. □

We now prove the main results of this paper.

**Theorem 5.8.** *Let $n \geqslant 10^{400}$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of $X_H$ is modular, hence we have*

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at 2,} \\ N'/H', & \text{otherwise,} \end{cases}$$

*where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.*

*Proof.* Let $\mathcal{N}$ be the normalizer of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$. By Proposition 5.6 we have

$$\mathcal{N}/\mathbb{P}(\Gamma_H) \cong \begin{cases} \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H) \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at 2,} \\ \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H), & \text{otherwise,} \end{cases}$$

where the first case is true because $\mathbb{P}(\gamma_1\gamma_0\Gamma_H)$ has order 2 in $\mathcal{N}/\mathbb{P}(\Gamma_H)$ and commutes with every element in $\mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H)$. Since $\mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H) \cong \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_{H'}) \cong N'/H'$, it is enough to prove that every automorphism of $X_H$ is modular. For $n \geqslant 10^{400}$ every automorphism is defined over the compositum of some quadratic fields by Proposition 4.7. We can bound the gonality $\mathrm{gon}(X_H)$ of $X_H$ using [Abr96] and, with the same estimates used in the proof of Proposition 3.12, we have

$$\mathrm{gon}(X_H) \geqslant \frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H] \geqslant \frac{7n^2}{800(\omega(n)+1)2^{\omega(n)}} > 10n.$$

So, there is at least one prime $\ell$ not dividing $n$ with $5 \leqslant \ell < \frac{1}{2}\mathrm{gon}(X_H)-1$. By Lemma 5.3, we can conclude that every automorphism is modular. □

*Remark* 5.9. One can determine the groups $N'/H'$ in all cases. Indeed, let $n = \prod_{i=1}^r p_i^{e_i}$ be any positive integer with its prime factorization, let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup and let $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ be the normalizer of the group $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. By Chinese Remainder Theorem we have

$$H' \cong \prod_{i=1}^r H_i' \quad \text{and} \quad N' \cong \prod_{i=1}^r N_i' \quad \text{inside} \quad \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{i=1}^r \mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z}),$$

where $H_i'$ is the image of $H'$ in $\mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z})$ and $N_i' < \mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z})$ is the normalizer of $H_i'$. Hence the knowledge of $N'/H'$ for $H \in \{C_{\mathrm{ns}}(p^e), C_{\mathrm{ns}}(p^e), C_{\mathrm{s}}(p^e), C_{\mathrm{s}}^+(p^e)\}$ allows to compute the group $N'/H'$ for every Cartan or Cartan-plus subgroup $H$ of level $n$ not necessarily a prime power. For the prime power cases see Lemma 5.10 and Table 5.1 below.

**Lemma 5.10.** *Let $e$ be a positive integer and let $p$ be a prime. Let $H < \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup and let $N' < \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ be the normalizer of the group $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$. Then:*

- *if $H = C_{\mathrm{ns}}(p^e)$, then $N'/H' \cong \mathbb{Z}/2\mathbb{Z}$, since $N' = C_{\mathrm{ns}}^+(p^e) \cap \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$;*
- *if $H = C_{\mathrm{ns}}^+(p^e)$ and $p^e \neq 3$, then $N'/H' \cong \{1\}$;*
- *if $H = C_{\mathrm{s}}(p^e)$ and $p \neq 2, 3$, then $N'/H' \cong \langle\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\rangle \cong \mathbb{Z}/2\mathbb{Z}$;*
- *if $H = C_{\mathrm{s}}^+(p^e)$ and $p \neq 2, 3$ and $p^e \neq 5$, then $N'/H' \cong \{1\}$.*

*The cases left out are listed in Table 5.1 below.*

*Proof.* It is a direct computation. □

Note that the groups $N'/H'$ computed for $H = C_{\mathrm{s}}(p^e)$ are the same determined in [AL70], [AS90], [Bar08], in the setting of Borel modular curves.

For Cartan modular curves of prime power level we make Theorem 5.8 more precise.

**Theorem 5.11.** *Let $p$ be a prime number and let $e$ be a positive integer. If $p^e > 11$ and $p^e \notin \{3^3, 2^4, 2^5, 2^6\}$, then all the automorphisms of $X_{\mathrm{ns}}(p^e)$, $X_{\mathrm{ns}}^+(p^e)$, $X_{\mathrm{s}}(p^e)$ and $X_{\mathrm{s}}^+(p^e)$ are*

TABLE 5.1. Automorphism groups.

| $H$ | $N'/H'$ | Generators | Comments |
|---|---|---|---|
| $C_{\mathrm{ns}}^+(3)$ | $\mathbb{Z}/3\mathbb{Z}$ | $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}(2^e)$<br>$1\leqslant e\leqslant 3$ | $\mathrm{PSL}_2(\mathbb{Z}/2^e\mathbb{Z})$ | $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$ | |
| $C_{\mathrm{s}}(2^4)$ | $D_8 \rtimes_\varphi (\mathbb{Z}/8\mathbb{Z})$<br>with<br>$(\varphi(1))\,(1,0) = (5,0)$<br>$(\varphi(1))\,(0,1) = (3,1)$ | $\left(\begin{smallmatrix}-1&6\\6&-5\end{smallmatrix}\right)$,$\left(\begin{smallmatrix}4&9\\7&-4\end{smallmatrix}\right)$ for $D_8$<br>and $\left(\begin{smallmatrix}1&-2\\0&1\end{smallmatrix}\right)$ for $\mathbb{Z}/8\mathbb{Z}$ | $D_8 \cong \mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is the dihedral group of order 16; $N'/H'$ is the group labeled as $(128,68)$ in MAGMA, [Gro] |
| $C_{\mathrm{s}}(2^e)$<br>$e \geqslant 5$ | $(\mathbb{Z}/8\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$<br>with $(\varphi(1))\,(x,y){=}(y,x)$ | $\left(\begin{smallmatrix}1&2^{e-3}\\0&1\end{smallmatrix}\right)$,$\left(\begin{smallmatrix}1&0\\-2^{e-3}&1\end{smallmatrix}\right)$ for $(\mathbb{Z}/8\mathbb{Z})^2$<br>and $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ for $\mathbb{Z}/2\mathbb{Z}$ | this group is labeled as $(128,67)$ in MAGMA, [Gro] |
| $C_{\mathrm{s}}(3)$ | $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z})$ | $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ | |
| $C_{\mathrm{s}}(3^e)$<br>$e \geqslant 2$ | $\mathbb{Z}/3\mathbb{Z} \times S_3$ | $\left(\begin{smallmatrix}1&3^{e-1}\\-3^{e-1}&1\end{smallmatrix}\right)$ for $\mathbb{Z}/3\mathbb{Z}$<br>and $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$,$\left(\begin{smallmatrix}1&3^{e-1}\\3^{e-1}&1\end{smallmatrix}\right)$ for $S_3$ | $S_3$ is the symmetric group acting on three elements |
| $C_{\mathrm{s}}^+(2)$ | $\{1\}$ | | |
| $C_{\mathrm{s}}^+(2^2)$ | $\mathbb{Z}/2\mathbb{Z}$ | $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}^+(2^3)$ | $\mathbb{Z}/4\mathbb{Z}$ | $\left(\begin{smallmatrix}1&-2\\2&-3\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}^+(2^4)$ | $\mathbb{Z}/8\mathbb{Z}$ | $\left(\begin{smallmatrix}1&6\\2&-3\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}^+(2^5)$ | $\mathbb{Z}/8\mathbb{Z}$ | $\left(\begin{smallmatrix}1&-4\\4&-15\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}^+(2^e)$<br>$e \geqslant 6$ | $\mathbb{Z}/8\mathbb{Z}$ | $\left(\begin{smallmatrix}1&-2^{e-3}\\2^{e-3}&1\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}^+(3)$ | $\mathbb{Z}/2\mathbb{Z}$ | $\left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}^+(3^e)$<br>$e \geqslant 2$ | $\mathbb{Z}/3\mathbb{Z}$ | $\left(\begin{smallmatrix}1&-3^{e-1}\\3^{e-1}&1\end{smallmatrix}\right)$ | |
| $C_{\mathrm{s}}^+(5)$ | $\mathbb{Z}/3\mathbb{Z}$ | $\left(\begin{smallmatrix}1&2\\1&3\end{smallmatrix}\right)$ | |

*modular and*

$$\mathrm{Aut}(X_{\mathrm{ns}}(p^e)) \cong \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{Aut}(X_{\mathrm{ns}}^+(p^e)) \cong \{1\},$$

$$\mathrm{Aut}(X_{\mathrm{s}}(p^e)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2,\\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3,\\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3,\end{cases} \quad \mathrm{Aut}(X_{\mathrm{s}}^+(p^e)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2,\\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3,\\ \{1\}, & \text{if } p > 3,\end{cases}$$

*where the above semidirect product* $(\mathbb{Z}/8\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ *is described in Table 5.1.*

*Proof.* We first treat the case $p^e > 49$ with $p^e \neq 2^6 = 64$. Up to conjugacy we can assume that $H \in \{C_{\mathrm{s}}(p^e), C_{\mathrm{s}}^+(p^e), C_{\mathrm{ns}}(p^e), C_{\mathrm{ns}}^+(p^e)\}$ where these groups are the subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ defined in Chapter 3 and $X_H \in \{X_{\mathrm{ns}}(p^e), X_{\mathrm{ns}}^+(p^e), X_{\mathrm{s}}(p^e), X_{\mathrm{s}}^+(p^e)\}$ is the corresponding associated modular curve. By [Abr96, Theorem 0.1] and Table 3.1, for

$p^e > 87$, we have the following lower bounds for the gonality of $X_H$:

$$\mathrm{gon}(X_H) \geqslant \frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H] \geqslant \frac{7}{800}\frac{p^{2e}(1-\frac{1}{p})}{2} > \frac{7 \cdot 87^2}{3200} > 16.$$

Hence either the prime $\ell = 5$ or the prime $\ell = 7$, are different from $p$, and satisfy $5 \leqslant \ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$. With a similar computation one can show that $\mathrm{gon}(X_H) > 12$, for $49 < p^e \leqslant 87$, if $p^e \neq 64$ and we can take $\ell = 5$. Applying Lemma 5.3 we deduce that all the automorphisms of $X_H$ defined over a compositum of quadratic fields are modular, hence, by Proposition 4.8, all the automorphisms of $X_H$ are modular. Finally, we can use Proposition 5.6, Lemma 5.10 and Remark 5.9 to obtain the group of modular automorphisms.

We now assume $11 < p^e \leqslant 49$. All the cases $X_{\mathrm{s}}(p^e) \cong X_0(p^{2e})$ are treated in [KM88], all the cases $X_{\mathrm{s}}^+(p)$ are treated in [Gon16] and the cases $X_{\mathrm{ns}}(p)$, $X_{\mathrm{ns}}^+(p)$, for $13 \leqslant p \leqslant 31$, are treated in [Gon17]. The remaining cases $X_{\mathrm{s}}^+(25)$, $X_{\mathrm{s}}^+(49)$ and $X_{\mathrm{ns}}(p^e)$, $X_{\mathrm{ns}}^+(p^e)$, for $p^e = 25, 37, 41, 43, 47, 49$, are treated in the MAGMA script available at [Scr]. □

Last theorem can be specialized to the prime level case, obtaining new results for non-split Cartan curves. The split cases are treated in [Gon16] and [KM88].

**Corollary 5.12.** *Let $p \geqslant 13$ be a prime number. Then the group of automorphisms of $X_{\mathrm{ns}}^+(p)$ is trivial and the group of automorphisms of $X_{\mathrm{ns}}(p)$ has order* 2.

*Remark* 5.13. Theorem 5.11 implies that, for $p^{2e}$ big enough, all the automorphisms of $X_0^*(p^{2e}) \cong X_{\mathrm{s}}^+(p^e)$ are modular, extending [BH03] and [Gon16] that treat the cases $X_0^*(p)$ and $X_0^*(p^2)$ and complementing in part [BG] which treats the case of $X_0^*(n)$ for $n$ squarefree. Our techniques (in particular Lemma 5.3) cannot be generalized to the case $X_0^*(p^e)$ with $e$ odd, because some branch points of the natural map $\mathbb{H} \to Y_0^+(p^e)$ have the form $\{(E, C), (E/C, E[p^e]/C)\}$ with $E \neq E_i, E_\rho$. Anyway, the techniques used in [Gon16, Lemmas 4, 5, 6], together with Proposition 4.9, can be used to prove the modularity of all elements in $\mathrm{Aut}(X_0^*(p^e))$, without restrictions on $e$, for all but finitely many cases.

It is a natural question to ask whether modular automorphisms such as those described in Lemma 5.10 are defined on a small field. The next proposition partially addresses this issue.

**Proposition 5.14.** *Let $n$ be a positive integer, let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$ and let $H' = H \cap SL_2(\mathbb{Z}/n\mathbb{Z})$. Let $M \in SL_2(\mathbb{Z})$ such that its reduction $M \bmod n$ normalizes $(H')^T$. Then $M$ defines a modular automorphism of $X_H$ which is defined over the cyclotomic field $\mathbb{Q}(\zeta_n)$. Moreover, this automorphism is defined over $\mathbb{Q}$ if and only if $M \bmod n$ normalizes $H^T$.*

*Proof.* Since $M$ normalizes $\Gamma_H$, it defines a modular automorphism $\Psi$ of $X_H$. From now on, we only look at the restriction of $\Psi$ to $Y_H$. Let $Y_{H'}^{cc}$ be the connected component of $Y_{H'}$ such that $Y_{H'}^{cc} = \Gamma_H \backslash \mathbb{H}$. Hence the natural map $Y_{H'} \to Y_H$ restricts to an isomorphism between $Y_{H'}^{cc}$ and $Y_H$ defined over $\mathbb{Q}(\zeta_n)$, which is also the field of definition of $Y_{H'}^{cc}$. The curve $Y_{H'}^{cc}/\mathbb{Q}(\zeta_n)$ can be interpreted as the coarse moduli space of elliptic curves with $H'$-structure $(E, \phi)$ such that the Weil pairing of $(\phi\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \phi\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right))$ is a fixed root of unity $\zeta$. Moreover, under the isomorphism $Y_H \cong Y_{H'}^{cc}$, we can describe $\Psi$ as

$$\Psi\colon Y_{H'}^{cc} \to Y_{H'}^{cc}, \quad (E, \phi) \mapsto (E, \phi \circ m), \tag{5.15}$$

with $m := M^{-T} \bmod n$. Since the map $(E,\phi) \mapsto (E, \phi \circ m)$ also defines a natural transformation between the functor coarsely represented by $Y_{H'}^{cc}$ and itself, we deduce that $\Psi$ is defined over $\mathbb{Q}(\zeta_n)$.

Notice that for every point $P \in Y_H(\mathbb{C})$ the image $\Psi(P)$ can be described by Equation (5.15) a priori only if we choose for $P$ a representative $(E,\phi)$ such that the Weil pairing of $(\phi\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \phi\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right))$ is $\zeta$.

We now prove that the map $\Psi$ is defined over $\mathbb{Q}$ if and only if $m$ normalizes the whole $H$. One implication is trivial, since, when $m$ normalizes $H$, the map $(E,\phi) \mapsto (E,\phi \circ m)$ also defines a natural transformation between the functor coarsely represented by $Y_H$ and itself. For the other implication, suppose that $m$ is in the normalizer of $H'$ but not in the normalizer of $H$ and let $h \in H$ be such that $m^{-1}hm \notin H$. Let $(E,\phi)$ be a point in $Y_{H'}^{cc}(\overline{\mathbb{Q}})$ such that $E$ is defined over $\mathbb{Q}$. Then, in $Y_H(\overline{\mathbb{Q}})$, for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$\sigma(E,\phi) = (E, \sigma \circ \phi) = (E, \sigma \circ \phi \circ h).$$

If we choose $\sigma$ such that $\sigma(\zeta_n) = \zeta_n^{\det h^{-1}}$, then the Weil pairing of $(\sigma \circ \phi \circ h\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \sigma \circ \phi \circ h\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right))$ is the same as the Weil pairing of $(\phi\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \phi\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right))$ which is equal to $\zeta$. Hence, we can use Equation (5.15) to deduce that

$$\begin{aligned} \sigma(\Psi(E,\phi)) &= \sigma(E, \phi \circ m) = (E, \sigma \circ \phi \circ m), \\ \Psi(\sigma(E,\phi)) &= \Psi(E, \sigma \circ \phi \circ h) = (E, \sigma \circ \phi \circ h \circ m). \end{aligned}$$

If $\Psi$ was defined over $\mathbb{Q}$, we would have $\sigma(\Psi(E,\phi)) = \Psi(\sigma(E,\phi))$, implying that $m^{-1}hm$ belongs to $H$ which is a contradiction. □

*Remark* 5.16. The proposition above, together with Theorem 5.11, implies that, given a prime power $p^e > 11$ not in $\{3^3, 2^4, 2^5, 2^6\}$, all the automorphisms of a Cartan curve of level $p^e$ are defined over the cyclotomic field $\mathbb{Q}(\zeta_{p^e})$. In general, not all such automorphisms are defined over $\mathbb{Q}$, even though this is true when the prime $p$ is at least 5 or when the Cartan group is non-split.

## 6. Appendix

**Characters of $\mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$.** Let $G := \mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$. For each $H < G$, let $\chi_H \colon G \to \mathbb{Q}$ be the character of the representation $\mathbb{Q}[G/H] = \bigoplus gH \cdot \mathbb{Q}$, computed using Equation (3.5). Every element of $G$ is conjugated to a unique element appearing in the first column, hence the table determines the characters $\chi_H$ for $H$ appearing in Proposition 3.3 or in [Che04, Theorem 1.1]. In the first column we have $\lambda, a \in (\mathbb{Z}/2^e\mathbb{Z})^\times$, $b \in (\mathbb{Z}/2^e\mathbb{Z})$, $k \in \{1, \dots, e-1\}$, and $u \in (\mathbb{Z}/2^{e-k}\mathbb{Z})^\times$.

Character table.

| | $B_r, r \geqslant 0$ | $T_0$ | $T_r, r > 0$ | $C_s$ | $C_s^+$ | $C_{\mathrm{ns}}$ | $C_{\mathrm{ns}}^+$ |
|---|---|---|---|---|---|---|---|
| $\lambda\mathrm{Id}$ | $3{\cdot}2^{2r}$ | 1 | $3{\cdot}2^{2r-1}$ | $3{\cdot}2^{2e-1}$ | $3{\cdot}2^{2e-2}$ | $2^{2e-1}$ | $2^{2e-2}$ |
| $\left(\begin{smallmatrix}0 & a\\ 1 & b\end{smallmatrix}\right)$<br>$b$ odd | 0 | 1 | 0 | 0 | 0 | 2 | 1 |
| $\left(\begin{smallmatrix}0 & a\\ 1 & b\end{smallmatrix}\right)$<br>$b$ even | 1 if $r{=}0$<br>0 if $r{>}0$ | 1 | 0 | 0 | $2^{e-1}$ if $b{=}0$<br>0 if $b{\neq}0$ | 0 | $2^{e-1}$ if $b{=}0$<br>0 if $b{\neq}0$ |
| $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda+2^k u\end{smallmatrix}\right)$ | $3{\cdot}2^{2r}$ if $r{<}k$<br>$2^{2k+1}$ if $r{\geqslant}k$ | 1 | $3{\cdot}2^{2r-1}$ if $r{\leqslant}k$<br>$2^{2k+1}$ if $r{>}k$ | $2^{2k+1}$ | $2^{2k}$ | 0 | 0 |
| $\left(\begin{smallmatrix}\lambda & 2^k u\\ 2^k & \lambda\end{smallmatrix}\right)$ | $3{\cdot}2^{2r}$ if $r{<}k$<br>$2^{2r}$ if $r{=}k$<br>0 if $r{>}k$ | 1 | $3{\cdot}2^{2r-1}$ if $r{\leqslant}k$<br>0 if $r{>}k$ | 0 | 0 | 0 | 0 |
| $\left(\begin{smallmatrix}\lambda & 2^k u\\ 2^k & \lambda+2^k\end{smallmatrix}\right)$ | $3{\cdot}2^{2r}$ if $r{<}k$<br>0 if $r{\geqslant}k$ | 1 | $3{\cdot}2^{2r-1}$ if $r{\leqslant}k$<br>0 if $r{>}k$ | 0 | 0 | $2^{2k+1}$ | $2^{2k}$ |
| $\left(\begin{smallmatrix}\lambda & 2^k u\\ 2^k & \lambda+2^{k+1}\end{smallmatrix}\right)$ | $3{\cdot}2^{2r}$ if $r{<}k$<br>$2^{2r}$ if $r{=}k$<br>0 if $r{>}k$ | 1 | $3{\cdot}2^{2r-1}$ if $r{\leqslant}k$<br>0 if $r{>}k$ | 0 | 0 | 0 | 0 |

**Data for Cartan modular curves of level $n \leqslant 64$.** In Table 6.1, we collect some relevant data about totally split or totally non-split Cartan modular curves of low level. Here $n$ is the level of the curve, $g$ is the genus, $\widetilde{\mathrm{cm}}$ is the dimension of the CM part after removing all factors isogenous to elliptic curves over $\mathbb{Q}$, and $A$ is the Abramovich's lower bound for the gonality of the curve (see [Abr96]). The values were computed through the script at [Scr] using the data on modular forms at [LMF21].

We write in *italic* the cases of genus 0 or 1: in these cases we know that there are infinitely many automorphisms which are not modular. We write in **bold** the cases where we have $\widetilde{\mathrm{cm}} < \frac{g-1}{2}$ and $A > 2(\ell{+}1)$ for some prime $\ell \geqslant 5$ not dividing $n$: in these cases we are able to prove that all the automorphisms are modular using Lemma 4.1 (we can apply it because of the first inequality) and Lemma 5.3 (we can apply it because of the second inequality). In the remaining cases we are not able to determine whether all the automorphisms are modular just by looking at $g$, $\widetilde{\mathrm{cm}}$ and $A$. We notice that in Theorem 5.8 we mostly use the hypothesis "$n \geqslant 10^{400}$" in order to conclude that the inequality $\widetilde{\mathrm{cm}} < \frac{g-1}{2}$ holds. On the other hand, one can check that the inequality $A > 2(\ell+1)$ holds starting from a much smaller $n$. When looking at explicit examples, we notice that, except for $X_{\mathrm{ns}}^{+}(48)$, in all the cases of genus at least 2 in the table, we have $\widetilde{\mathrm{cm}} < \frac{g-1}{2}$ and this implies that all the automorphisms are defined over a compositum of quadratic fields.

*Remark* 6.1. We highlight two interesting examples with exceptional automorphisms. The modular curves $X_{\mathrm{ns}}^{+}(16)$ and $X_{\mathrm{ns}}^{+}(20)$ have genus two, and hence they are hyperelliptic. An equation for both curves and the description of all rational points can be found in [Bar10, Section 5]. We computed the automorphism group of both curves using the built-in function in MAGMA: the automorphism group of $X_{\mathrm{ns}}^{+}(16)$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ while the automorphism group of $X_{\mathrm{ns}}^{+}(20)$ is $\mathbb{Z}/2\mathbb{Z}$. All the non-trivial automorphisms are exceptional. Furthermore, in the case of $X_{\mathrm{ns}}^{+}(16)$ the exceptional automorphisms give a non-CM rational point.

Table 6.1. Data for low level cases.

| | $X_{\mathrm{ns}}^{+}(n)$ | | | $X_{\mathrm{ns}}(n)$ | | | $X_{\mathrm{s}}^{+}(n)$ | | | $X_{\mathrm{s}}(n)$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $n$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ |
| 1 | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* |
| 2 | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* |
| 3 | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* |
| 4 | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* |
| 5 | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* | *0* | *0* | *1* |
| 6 | *0* | *0* | *1* | *1* | *0* | *1* | *0* | *0* | *1* | *1* | *0* | *1* |
| 7 | *0* | *0* | *1* | *1* | *0* | *1* | *0* | *0* | *1* | *1* | *0* | *1* |
| 8 | *0* | *0* | *1* | *1* | *0* | *1* | *1* | *0* | *1* | 3 | 0 | 1 |
| 9 | *0* | *0* | *1* | 2 | 0 | 1 | *1* | *0* | *1* | 4 | 0 | 1 |
| 10 | *0* | *0* | *1* | *1* | *0* | *1* | *1* | *0* | *1* | 7 | 0 | 2 |
| 11 | *1* | *0* | *1* | 4 | 0 | 1 | 2 | 0 | 1 | 6 | 0 | 2 |
| 12 | *0* | *0* | *1* | 3 | 0 | 1 | 3 | 0 | 2 | 13 | 0 | 3 |
| 13 | 3 | 0 | 1 | 8 | 0 | 2 | 3 | 0 | 1 | 8 | 0 | 2 |
| 14 | *0* | *0* | *1* | 5 | 0 | 1 | 3 | 0 | 2 | 17 | 0 | 3 |
| 15 | *1* | *0* | *1* | 7 | 2 | 2 | 4 | 0 | 2 | 19 | 2 | 4 |
| 16 | 2 | 0 | 1 | 7 | 2 | 2 | 9 | 0 | 2 | 21 | 2 | 4 |
| 17 | 6 | 0 | 2 | 15 | 0 | 3 | 7 | 0 | 2 | 17 | 0 | 3 |
| 18 | *0* | *0* | *1* | 7 | 0 | 1 | 7 | 0 | 3 | 37 | 0 | 6 |
| 19 | 8 | 0 | 2 | 20 | 0 | 3 | 9 | 0 | 2 | 22 | 0 | 4 |
| 20 | 2 | 0 | 1 | 9 | 0 | 2 | 10 | 0 | 4 | 43 | 0 | 7 |
| 21 | *1* | *0* | *2* | 15 | 2 | 3 | 9 | 0 | 3 | 41 | 2 | 6 |
| 22 | *1* | *0* | *1* | 13 | 2 | 2 | 10 | 0 | 4 | 49 | 2 | 7 |
| 23 | 13 | 0 | 3 | 31 | 3 | 5 | 15 | 0 | 3 | 35 | 3 | 5 |
| 24 | *1* | *0* | *1* | 13 | 0 | 2 | 17 | 0 | 6 | 73 | 0 | 11 |
| 25 | 14 | 0 | 3 | 32 | 0 | 5 | 22 | 0 | 4 | 48 | 0 | 7 |
| 26 | 3 | 0 | 2 | 21 | 0 | 3 | 15 | 0 | 5 | 71 | 0 | 10 |
| 27 | 12 | 0 | 3 | 32 | 0 | 5 | 28 | 0 | 5 | 64 | 0 | 9 |
| 28 | 4 | 0 | 2 | 23 | 0 | 3 | 21 | 0 | 6 | 89 | 0 | 12 |
| 29 | 24 | 0 | 4 | 54 | 0 | 8 | 26 | 0 | 4 | 58 | 0 | 8 |
| 30 | *1* | *0* | *2* | 17 | 2 | 3 | 16 | 0 | 10 | **145** | **6** | **19** |
| 31 | 28 | 0 | 5 | 63 | 3 | 9 | 30 | 0 | 5 | 67 | 3 | 9 |
| 32 | 14 | 2 | 3 | 35 | 3 | 5 | 49 | 8 | 7 | **105** | **18** | **14** |

| | $X_{\mathrm{ns}}^{+}(n)$ | | | $X_{\mathrm{ns}}(n)$ | | | $X_{\mathrm{s}}^{+}(n)$ | | | $X_{\mathrm{s}}(n)$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $n$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ | $g$ | $\widetilde{\mathrm{cm}}$ | $A$ |
| 33 | 7 | 2 | 3 | 45 | 2 | 6 | 25 | 2 | 7 | **109** | **2** | **14** |
| 34 | 6 | 0 | 3 | 37 | 0 | 5 | 28 | 0 | 9 | **127** | **0** | **17** |
| 35 | 13 | 0 | 4 | 59 | 6 | 8 | 27 | 0 | 8 | 117 | 6 | 15 |
| 36 | 5 | 0 | 2 | 31 | 0 | 4 | 43 | 0 | 12 | **181** | **0** | **23** |
| 37 | 43 | 0 | 6 | 94 | 0 | 12 | 45 | 0 | 7 | **98** | **0** | **13** |
| 38 | 8 | 0 | 3 | 49 | 2 | 6 | 36 | 0 | 10 | **161** | **2** | **20** |
| 39 | 13 | 0 | 5 | 67 | 6 | 9 | 36 | 0 | 10 | **155** | **6** | **20** |
| 40 | 10 | 0 | 3 | 45 | 4 | 6 | 49 | 0 | 13 | **205** | **12** | **26** |
| 41 | 54 | 0 | 8 | **117** | **0** | **15** | 57 | 0 | 8 | **123** | **0** | **16** |
| 42 | *1* | *0* | *3* | 37 | 2 | 5 | **33** | **0** | **18** | **289** | **6** | **36** |
| 43 | 60 | 0 | 8 | **130** | **0** | **16** | 63 | 0 | 9 | **136** | **0** | **17** |
| 44 | 13 | 0 | 4 | 63 | 4 | 8 | **55** | **2** | **14** | **229** | **8** | **28** |
| 45 | 17 | 0 | 5 | 79 | 2 | 10 | 55 | 0 | 15 | **235** | **14** | **29** |
| 46 | 13 | 0 | 5 | 73 | 3 | 9 | **55** | **0** | **15** | **241** | **9** | **29** |
| 47 | 73 | 0 | 10 | **157** | **5** | **19** | 77 | 0 | 10 | **165** | **5** | **20** |
| 48 | 9 | 4 | 4 | 57 | 16 | 7 | **81** | **4** | **21** | **337** | **20** | **41** |
| 49 | 69 | 0 | 10 | **151** | **0** | **19** | **94** | **6** | **13** | **201** | **12** | **25** |
| 50 | 14 | 0 | 5 | 73 | 0 | 9 | **77** | **0** | **20** | **331** | **0** | **40** |
| 51 | 25 | 5 | 8 | **121** | **8** | **15** | **64** | **5** | **17** | **271** | **8** | **33** |
| 52 | 21 | 0 | 6 | 93 | 0 | 11 | **78** | **0** | **20** | **323** | **0** | **39** |
| 53 | **96** | **0** | **13** | **204** | **0** | **25** | **100** | **0** | **13** | **212** | **0** | **26** |
| 54 | 12 | 0 | 5 | 73 | 0 | 9 | **100** | **0** | **26** | **433** | **0** | **52** |
| 55 | 38 | 0 | 10 | **163** | **6** | **20** | **70** | **0** | **18** | **295** | **6** | **35** |
| 56 | 21 | 0 | 6 | **101** | **4** | **12** | **97** | **4** | **24** | **401** | **12** | **48** |
| 57 | 31 | 5 | 9 | **153** | **8** | **18** | **81** | **5** | **20** | **341** | **8** | **40** |
| 58 | 24 | 0 | 8 | **121** | **0** | **15** | **91** | **0** | **23** | **391** | **0** | **46** |
| 59 | **121** | **3** | **15** | **256** | **3** | **30** | **126** | **3** | **16** | **266** | **3** | **31** |
| 60 | 7 | 0 | 5 | 73 | 4 | 9 | **79** | **0** | **38** | **649** | **12** | **76** |
| 61 | **131** | **0** | **17** | **276** | **0** | **33** | **135** | **0** | **17** | **284** | **0** | **34** |
| 62 | 28 | 0 | 9 | **141** | **3** | **17** | **105** | **0** | **27** | **449** | **9** | **53** |
| 63 | 35 | 0 | 10 | **171** | **10** | **20** | **109** | **0** | **27** | **457** | **14** | **53** |
| 64 | 70 | 6 | 9 | **155** | **14** | **18** | **225** | **30** | **27** | **465** | **62** | **54** |

## References

[Abr96] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011. MR 1422373

[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160. MR 268123

[AS90] M. Akbas and D. Singerman, *The normalizer of* $\Gamma_0(N)$ *in* $\mathrm{PSL}(2,\mathbf{R})$, Glasgow Math. J. **32** (1990), no. 3, 317–327. MR 1073672

[Bar08] F. Bars, *The group structure of the normalizer of* $\Gamma_0(N)$ *after Atkin-Lehner*, Comm. Algebra **36** (2008), no. 6, 2160–2170. MR 2418382

[Bar09] B. Baran, *A modular curve of level 9 and the class number one problem*, J. Number Theory **129** (2009), no. 3, 715–728. MR 2488598

[Bar10] ———, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772. MR 2684496 (2011i:11083)

[Bar14] ———, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300.

[BCFS] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel, *Handbook of magma functions*, `http://magma.maths.usyd.edu.au/magma/handbook/`.

[BDM$^+$19] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944. MR 3961086

[BG] F. Bars and J. González, *The automorphism group of the modular curve* $X_0^*(N)$ *with square-free level*, Trans. Amer. Math. Soc., to appear.

[BH03] M. Baker and Y. Hasegawa, *Automorphisms of* $X_0^*(p)$, J. Number Theory **100** (2003), no. 1, 72–87. MR 1971247 (2004c:11100)

[BP11] Y. Bilu and P. Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584. MR 2753610 (2012a:11077)

[BPR13] Y. Bilu, P. Parent, and M. Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. MR 3137477

[Che98] I. Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 1–38. MR 1625491 (99m:11068)

[Che04] ———, *Jacobians of modular curves associated to normalizers of Cartan subgroups of level* $p^n$, C. R. Math. Acad. Sci. Paris **339** (2004), no. 3, 187–192. MR 2078072

[DFGS14] V. Dose, J. Fernández, J. González, and R. Schoof, *The automorphism group of the non-split Cartan modular curve of level 11*, J. Algebra **417** (2014), 95–102. MR 3244639

[DMS19] V. Dose, P. Mercuri, and C. Stirpe, *Double covers of Cartan modular curves*, J. Number Theory **195** (2019), 96–114. MR 3867436

[Dos16] V. Dose, *On the automorphisms of the nonsplit Cartan modular curves of prime level*, Nagoya Math. J. **224** (2016), no. 1, 74–92. MR 3572750

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR 0337993 (49 #2762)

[DS05] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196 (2006f:11045)

[dSE00] B. de Smit and B. Edixhoven, *Sur un résultat d'Imin Chen*, Math. Res. Lett. **7** (2000), no. 2-3, 147–153. MR 1764312 (2001j:11043)

[Elk90] N. D. Elkies, *The automorphism group of the modular curve* $X_0(63)$, Compositio Math. **74** (1990), no. 2, 203–208. MR 1047740 (91e:11064)

[GGJ05] D. Goldstein, R. Guralnick, and D. Joyner, *A question about* $\mathrm{Pic}(X)$ *as a G-module*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 232–242. MR 2182042

[Gon16] J. González, *Automorphism group of split Cartan modular curves*, Bull. Lond. Math. Soc. **48** (2016), no. 4, 628–636. MR 3532138

[Gon17] ———, *Constraints on the automorphism group of a curve*, J. Théor. Nombres Bordeaux **29** (2017), no. 2, 535–548. MR 3682478

[Gro] *Database of finite groups of small order*, `http://groupnames.org`.

[Har11] M. C. Harrison, *A New Automorphism Of* $X_0(108)$, arXiv:1108.5595 (2011).

[Ivi77] A. Ivić, *Two inequalities for the sum of divisors functions*, Univ. u Novom Sadu Zb. Rad. Prirod.-Mat. Fak. **7** (1977), 17–22.

[KM88] M. A. Kenku and F. Momose, *Automorphism groups of the modular curves $X_0(N)$*, Compositio Math. **65** (1988), no. 1, 51–80. MR 930147 (88m:14015)

[LMF21] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, 2021, [Online; accessed 5 June 2021].

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230 (80h:14022)

[Mer18] P. Mercuri, *Equations and rational points of the modular curves $X_0^+(p)$*, Ramanujan J. **47** (2018), no. 2, 291–308. MR 3863642

[MS20] P. Mercuri and R. Schoof, *Modular forms invariant under non-split cartan subgorups*, accepted by Mathematics of Computation (2020).

[Nar04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Monographs in Mathematics, Springer Berlin Heidelberg, 2004.

[NR83] J.-L. Nicolas and G. Robin, *Majorations explicites pour le nombre de diviseurs de n*, Canadian Mathematical Bulletin **26** (1983), no. 4, 485–492.

[Ogg75a] A. P. Ogg, *Automorphismes de courbes modulaires*, Séminaire Delange-PisotPoitou (16e année: 1974/75), Théorie des nombres, Fasc. 1, Exp. No. 7, 1975, p. 8. MR 0417184

[Ogg75b] Andrew P Ogg, *Diophantine equations and modular forms*, Bulletin of the American Mathematical Society **81** (1975), no. 1, 14–27.

[Ogg77] A. P. Ogg, *Über die Automorphismengruppe von $X_0(N)$*, Math. Ann. **228** (1977), no. 3, 279–292. MR 0562500 (58 #27775)

[Rob83a] G. Robin, *Estimation de la fonction de tchebychef $\theta$ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega$ (n) nombre de diviseurs premiers de n*, Acta Arithmetica **42** (1983), no. 4, 367–389.

[Rob83b] ———, *Grandes valeurs de fonctions arithmétiques et problèmes d'optimisation en nombres entiers*, Ph.D. thesis, 1983.

[RS62] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics **6** (1962), no. 1, 64–94.

[Scr] *Magma shared code*, `https://github.com/guidoshore/automorphisms_of_Cartan_modular_curves`, Accessed: 2020-04-04.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR 0387283 (52 #8126)

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR 1757192

[Shi71a] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971, Kanô Memorial Lectures, No. 1. MR 0314766

[Shi71b] ———, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208. MR 0296050 (45 #5111)

[Shi72] ———, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. (2) **95** (1972), 130–190. MR 0314801 (47 #3351)

*Email address*: `valerio.dose@uniroma1.it`

Dipartimento di Ingegneria Informatica Automatica e Gestionale, "Sapienza" Università di Roma, Via Ariosto 25, 00185 Roma, Italy

*Email address*: `guidomaria.lido@gmail.com`

Università "Tor Vergata", Rome 00133, Italy

*Email address*: `mercuri.ptr@gmail.com`

Università "Sapienza", Rome 00161, Italy